INSTALLATION GUIDE

WebShield e500 Appliance

VERSION 2.5

English/Deutsch/Français/ **日本語**

McAfee SECURITY

Contents

Ports and connectors vii
Mounting kit instructions viii
User interface x

Installation Guide — English ENG-1

Overview ENG-1
Copyright and trademark attributions ENG-2
Power and safety information ENG-3
About the WebShield e500 Appliance ENG-5
Features ENG-6
What comes with the appliance? ENG-10
Getting started with the appliance ENG-13
Who should install the appliance? ENG-13
Ports and connectors ENG-14
Gathering the configuration information ENG-18
Installing the appliance ENG-28
Configuring the network settings ENG-32
Configuring the protocol settings ENG-40
Configuring the appliance's protocols ENG-41
Configuring the automatic updating feature ENG-47
Configuring your other equipment ENG-48
Testing your configuration ENG-50
Using the appliance ENG-53
Backing up and restoring your settings ENG-55
Restoring and upgrading the appliance's software ENG-57
Troubleshooting ENG-60
Hardware problems ENG-60
User interface problems ENG-63

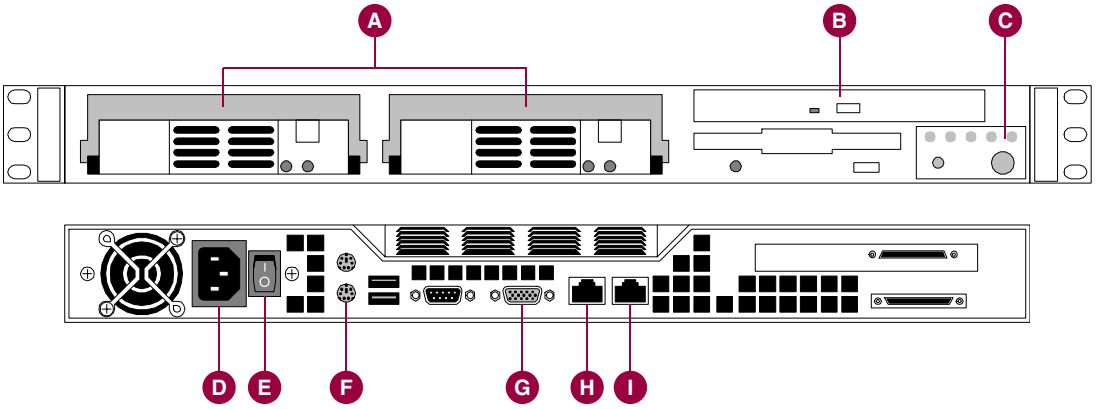
Installationshandbuch – Deutsch DEU-1

Übersicht DEU-1
Copyright und Marken DEU-2
Informationen zu Stromversorgung und Sicherheit DEU-3
Infos zu WebShield e500 . . . . . DEU-5
Funktionen DEU-6
Lieferumfang des WebShield e500 . . . . . DEU-11
Erste Schritte mit dem Gerät DEU-14
Wer das Gerät installieren sollte DEU-14
Ports und Stecker DEU-15
Zusammenfassen der Konfigurationsinformationen DEU-20
Installation des McAfee WebShield e500 . . . . . DEU-32
Konfigurieren der Netzwerkeinstellungen DEU-36
Konfigurieren der Protokolleinstellungen DEU-45
Konfigurieren der Protokolle des WebShield e500 . . . . . DEU-46
Konfigurieren der Funktion zum automatischen Aktualisieren . . DEU-52
Konfigurieren weiterer Geräte DEU-53
Testen Ihrer Konfiguration DEU-55
Verwenden des WebShield e250 . . . . . DEU-59
Sichern und Wiederherstellen der Einstellungen DEU-61
Wiederherstellen und Aktualisieren der Gerätesoftware DEU-64
Fehlerbehebung DEU-68
Hardwarefehler DEU-68
Probleme mit der Benutzeroberfläche DEU-71

Guide d'installation – Français FRA-1
Présentation FRA-1
Copyright et attribution de marques commerciales FRA-2
Informations sur l'alimentation et la sécurité FRA-3
A propos de l'application WebShield e500 . . . . . FRA-5
Fonctionnalités FRA-6
Contenu fourni avec l'application FRA-10
Mise en route de l'application FRA-13
Installateur de l'application FRA-13
Ports et connecteurs FRA-14
Collecter les informations de configuration FRA-19
Installation de l'application FRA-31
Configuration des paramètres réseau FRA-35
Configuration des paramètres de protocole FRA-45
Configuration des protocoles de l'application FRA-46
Configuration de la fonctionnalité de mise à jour automatique . FRA-52
Configuration des autres équipements FRA-53
Tester votre configuration FRA-55
Utilisation de l'application FRA-59
Sauvegarde et restauration de vos paramètres FRA-61
Restauration et mise à niveau du logiciel de l'application FRA-63
Dépannage FRA-67
Problèmes matériels FRA-67
Problèmes d'interface utilisateur FRA-70

インストール ガイド ー 日本語 ..... 日本語 - 1
概要 ..... 日本語 - 1
著作権と商標 ..... 日本語 - 2
電源および安全に関する情報 ..... 日本語 - 3
WebShield e500 アプライアンスについて ..... 日本語 - 5
製品の特色 ..... 日本語 - 6
パッケージの内容 ..... 日本語 - 10
アプライアンスの準備 ..... 日本語 - 13
インストールに必要なスキル ..... 日本語 - 13
ポートとコネクタ ..... 日本語 - 14
設定情報の収集 ..... 日本語 - 19
アプライアンスのインストール ..... 日本語 - 31
ネットワーク構成の設定 ..... 日本語 - 35
プロトコルの設定 ..... 日本語 - 43
プロトコルの設定 ..... 日本語 - 44
自動アップデートの設定 ..... 日本語 - 50
他の機器の設定 ..... 日本語 - 51
設定のテスト ..... 日本語 - 53
アプライアンスの使用方法 ..... 日本語 - 57
設定のバックアップと復元 ..... 日本語 - 59
ソフトウェアの復元とアップグレード ..... 日本語 - 61
トラブルシューティング ..... 日本語 - 65
ハードウェアに関する問題 ..... 日本語 - 65
ユーザ インターフェースに関する問題 ..... 日本語 - 67

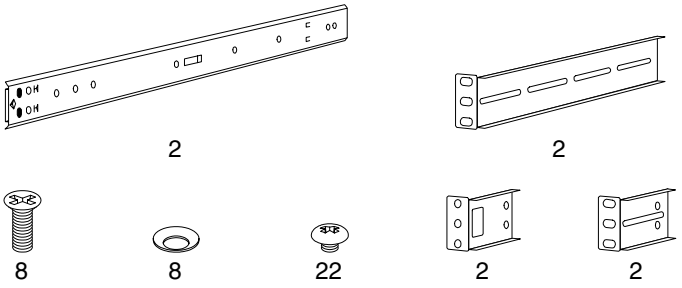
Ports and connectors
Ports und Stecker
Ports et connecteurs
ポートとコネクタ



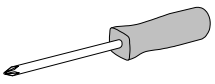
A	Two hard disk drives	Zwei Festplattenlaufwerke	Deux unités de disque dur	ハードディスク 2 個
B	CD-ROM drive	CD-ROM-Laufwerk	Lecteur CD-ROM	CD-ROM ドライブ
C	Control panel	Bedienungsfeld	Panneau de contrôle	コントロール パネル
D	Power socket	Netzanschluß	Prise d'alimentation	電源ソケット
E	Power supply switch	Stromversorgungsschalter	Interrupteur d'alimentation électrique	電源スイッチ
F	Keyboard port	Tastatur-Port	Port clavier	キーボード ポート
G	Monitor port	Monitor-Port	Port écran	モニタ ポート
H	LAN1 port (NIC 1)	LAN1-Port (NIC 1)	Port réseau local 1 (carte réseau 1)	LAN1 ポート (NIC 1)
I	LAN2 port (NIC 2)	LAN2-Port (NIC 2)	Port réseau local 1 (carte réseau 2)	LAN2 ポート (NIC 2)

Mounting kit instructions
Anweisungen für den Montagerahmen
Instructions de montage
マウントキットの組み立て方

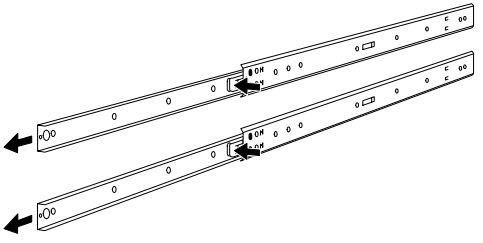
Supplied:
Im Lieferumfang:
Fourni:
同梱されている部品 :



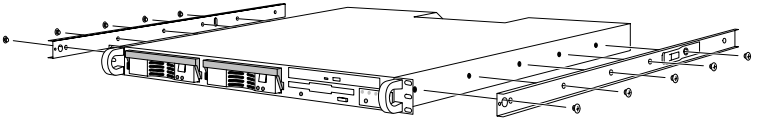
Required:
Zusätzlich erforderlich:
Requis:
必要な工具 :



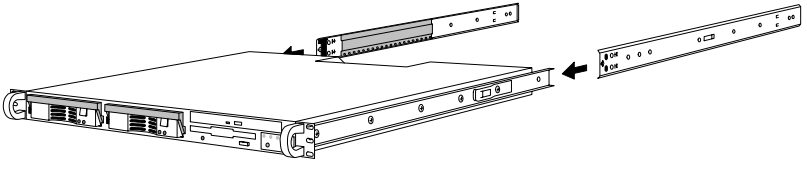
1



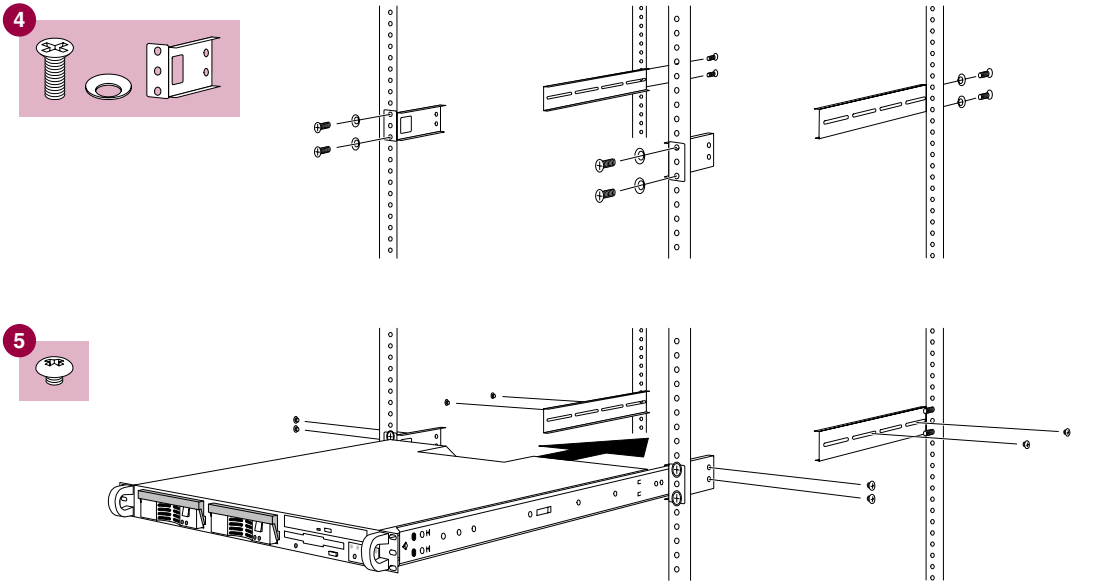
2



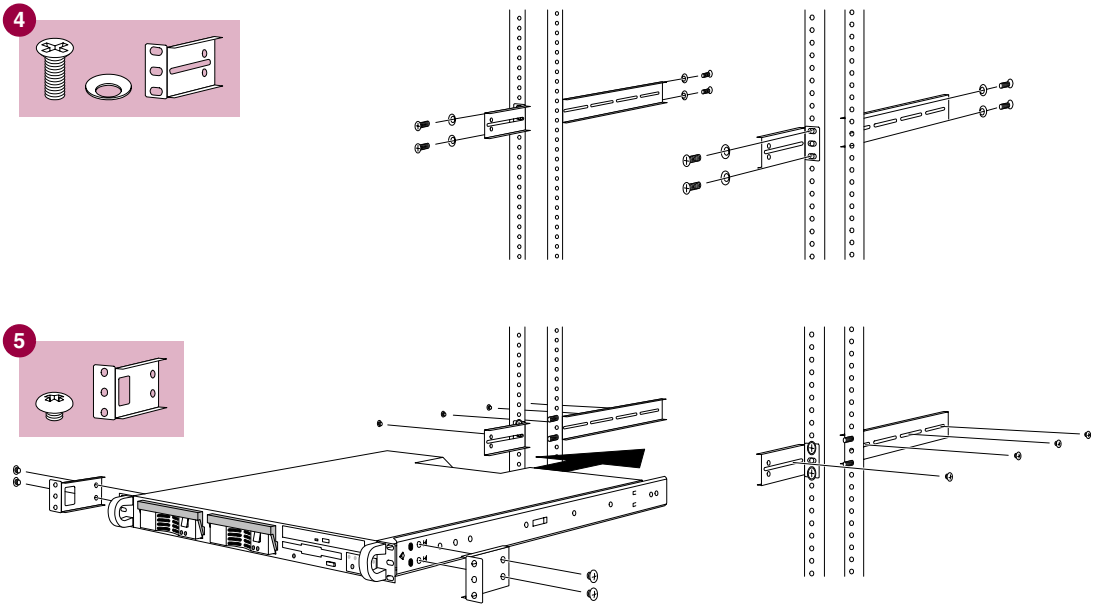
3



Standard rack / Standardgestell/Rack standard / 標準ラック：

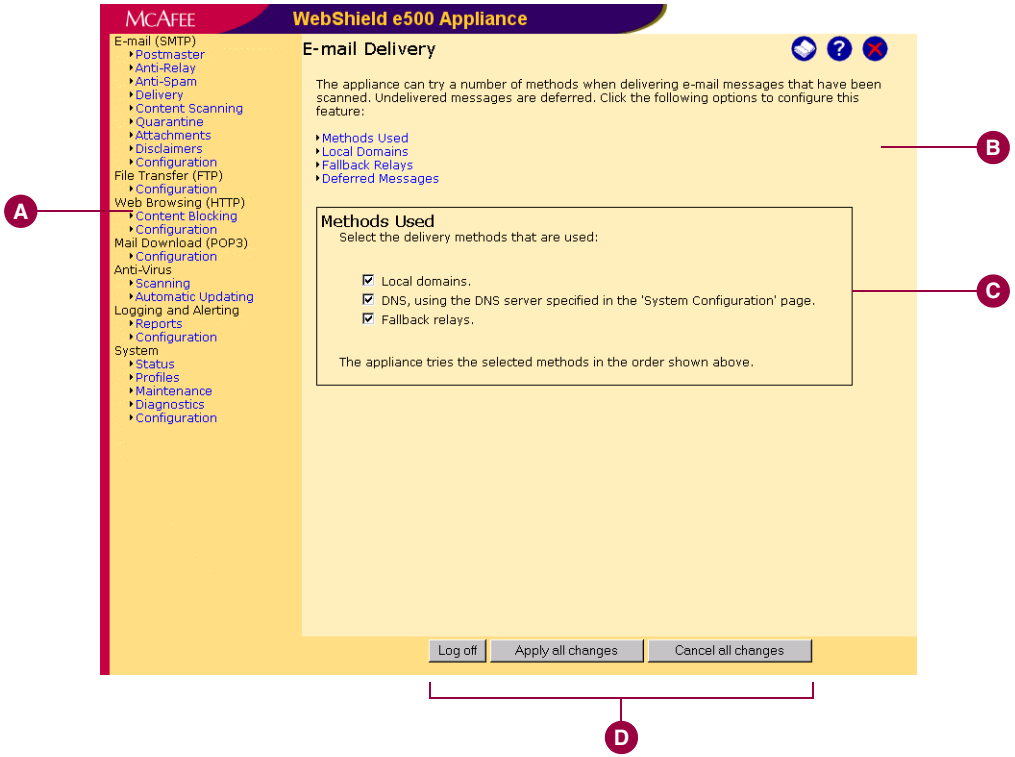


Telco rack / Telco-Gestell / Rack Telco/ Telco 社製ラック：



User interface
Benutzeroberfläche
Interface utilisateur
ユーザ インターフェース

Your user interface might look slightly different depending on the version and language.
Ihre Benutzeroberfläche kann je nach Version und Sprache anders aussehen.
L'interface utilisateur peut présenter de légères différences selon la version et la langue utilisées.
使用する言語とバージョンによって、インターフェースの外観が多少異なる場合があります。



A	Navigation bar	Navigationsleiste	Barre de navigation	ナビゲーション バー
B	Page	Seite	Page	ページ
C	Panel	Dialogfeld	Panneau	ペイン
D	Control buttons	Steuerungsschaltflächen	Boutons de contrôle	コントロール ボタン

Installation Guide — English

Overview

This Installation Guide provides the information you need to install and configure your WebShield appliance. Please refer to the following sections for specific information:

Copyright and trademark attributions **Page 2**

Power and safety information **Page 3**

About the WebShield e500 Appliance **Page 5**

- Features Page 6
- What comes with the appliance? Page 10

Getting started with the appliance **Page 13**

- Who should install the appliance? Page 13
- Ports and connectors Page 14
- Gathering the configuration information Page 18

Installing the appliance **Page 28**

Configuring the network settings **Page 32**

Configuring the protocol settings **Page 40**

- Configuring the appliance's protocols Page 41
- Configuring the automatic updating feature Page 47
- Configuring your other equipment Page 48
- Testing your configuration Page 50

Using the appliance **Page 53**

- Backing up and restoring your settings Page 55
- Restoring and upgrading the appliance's software Page 57

Troubleshooting **Page 60**

- Hardware problems Page 60
- User interface problems Page 63

Copyright and trademark attributions

COPYRIGHT

© 2001–2002 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 3965 Freedom Circle, Santa Clara, California 95054, or call +1-972-308-9960.

TRADEMARK ATTRIBUTIONS

Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, CyberCop, CyberCop (in Katakana), CyberMedia, CyberMedia UnInstaller, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, ISDN TEL/SCOPE, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctupus, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PC Medic 97, PCNotary, PGP, PGP (Pretty Good Privacy), Pretty Good Privacy, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, RingFence, Router PM, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SniffMaster, SniffMaster (in Hangul), SniffMaster (in Katakana), SniffNet, Stalker, SupportMagic, TIS, TMEG, TNV, TVD, TNS, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Power and safety information

IMPORTANT: To ensure safe operation of the WebShield e500 Appliance, read all of the following information carefully *before* installing the appliance.

Power requirements

- Ensure that the power cord is suitable for the country of use. If it is not suitable, contact your supplier. Do not attempt to modify the power cord.
- The power outlet to which you connect the appliance must meet all applicable electrical standards for the country of use.
- When connecting the appliance to the power outlet and other equipment, ensure that the cables are stowed or grouped safely, so that no one will trip over them.

Using the appliance

- Do not open the appliance's case. There are no user-serviceable parts inside.
- The appliance is heavy. When you lift it, ensure that you have a firm grip and carry it correctly, so that you do not injure yourself or damage the appliance.
- Place the appliance on a flat sturdy surface, such as a desk, or secure it in a rack, such as a 19" (inch) rack. Ensure that the surface or rack can support the weight of the appliance, and that it cannot fall.
- Do not place any heavy objects on top of the appliance.
- The appliance's network ports are only suitable for use with RJ-45 connectors. Do not use them with telephone equipment unless the socket to which you are connecting is specifically intended for 10Mbps or 100Mbps Ethernet network use.
- In the unlikely event that the appliance encounters a hardware failure, turn off the appliance and disconnect it from the power outlet. Contact your supplier.

Operating conditions

- Ensure that the environmental conditions surrounding the appliance are suitable for standard computer use. Check that it is not damp, with adequate ventilation. The operating temperature must remain within 10–40°C, and the humidity within 0–90%. If these values are exceeded, the appliance could fail to operate.
- When you use the appliance, ensure that there is a gap of at least 1" (25mm) behind the case, so that the appliance can cool itself properly.
- Ensure that liquid and other objects do not enter the appliance through its ventilation holes or fan grill.

About the WebShield e500 Appliance

The WebShield e500 Appliance (Figure 1-1) is a purpose-built anti-virus and content-scanning server containing powerful WebShield software. It is fully configurable through a web browser, and it can be used in almost any network topology. It provides virus scanning for the following protocols:

- Simple Mail Transfer Protocol (SMTP) e-mail messages
- File Transfer Protocol (FTP) exchanges
- Hypertext Transfer Protocol (HTTP) web browsing
- Post Office Protocol version 3 (POP3) Internet e-mail messages

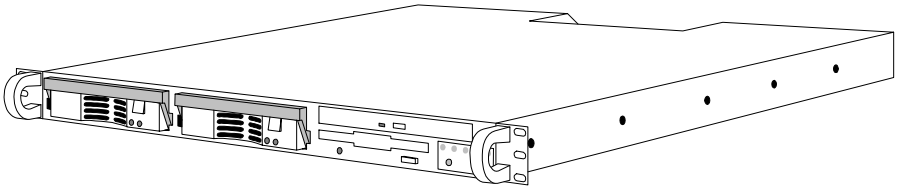


Figure 1-1. WebShield e500 Appliance

With additional features such as content scanning, anti-relay and anti-spam, the appliance provides complete protection for your Internet gateway, preventing undesirable material entering and leaving your organization.

The WebShield e500 Appliance shares its resources between the protocols that it scans, checking inbound and outbound traffic as required. It can detect, clean, log, and quarantine infected e-mail items, including compressed files and macros, preventing them from reaching their intended recipients. It can also block infected HTTP, FTP and POP3 items.

Using the appliance to perform your anti-virus scanning allows your mail server to remain dedicated to mail activities. You can also use multiple WebShield e500 Appliances together to increase scanning throughput and provide fault tolerance.

For details of the different ways to use the appliance and some example topologies, refer to Chapter 1 of the Product Guide.

Features

Transparency — a new feature for version 2.5

If you have used a previous version of the WebShield appliance, be aware that a new feature for version 2.5 is the addition of transparency. This means that you can now use the appliance in either *proxy mode* or *transparency mode*:

- **Proxy mode** (explicit proxy) is suitable for networks where you can easily configure your equipment to route its protocol traffic through the appliance. Before transparency was introduced, the appliance only operated in proxy mode.

  In proxy mode, the appliance only handles traffic for the protocols that it proxies.

- **Transparency mode** (transparent proxy) allows you to slot the appliance into networks where it is difficult or time-consuming to reconfigure your other equipment. The appliance then sits transparently on the network using static and dynamic routing information to receive and pass on the traffic that it scans.

  > **NOTE:** In transparency mode, the appliance must be connected to two different subnets (through its LAN1 and LAN2 ports).

  The appliance handles all IP traffic flowing between the two subnets.

For more details about these modes, see the "Proxy or transparency?" section in the Product Guide.

> **IMPORTANT:** Both modes are different so it is important that you understand and decide which mode you want to use *before* you install and configure the appliance.

For details on configuring the appliance with a configuration file taken from an earlier version of the appliance, see "Restoring your settings" on page 56.

Some of the appliance's other features are summarized in the remainder of this section.

Hardware

The appliance has many features, including the following:

- 1U high 19" (inch) rack-mountable hardware.
- Dual Intel Pentium III 1GHz processors.
- 256MB of PC133 SDRAM.
- Two RJ-45 10/100Mbps auto-sensing Ethernet network ports, allowing flexible connection to your existing network and a dedicated management interface (only available in proxy mode).
- Two 17.4GB "hot-pluggable" SCSI hard disk drives managed in a hardware-based RAID 1 (mirror) configuration. This ensures seamless processing in the unlikely event of a problem with one of the drives. When you insert a replacement drive, the RAID controller re-mirrors the new drive automatically.

For details on the appliance's ports and connectors, see page 14.

Software

The software on the appliance has the following features:

- Web management through Secure Sockets Layer (SSL) encryption from a web browser.
- An easy-to-configure user interface, allowing you to set up the appliance quickly. The appliance then requires minimal user-intervention, making it a configure-and-forget solution.
- Flexible proxies that are simple to configure even in complex environments; see "Gathering the configuration information" on page 18.
- Virus scanning of SMTP e-mail messages, checking for infected items and banned content. Other SMTP features include:
  - Flexible SMTP e-mail delivery configurations, allowing you to set up multiple e-mail delivery methods and introduce fault tolerance.
  - Flexible content scanning of messages, allowing you to search for banned content and block specific attachment types.
  - Spam blocking (rejecting unwanted e-mail messages) by recipient, sender, or server.

  - Support for real-time Blackhole lists, which identify potential sources of spam messages. The appliance can use these lists to block spam messages. Blackhole lists are available from many organizations, including the Mail Abuse Prevention System (MAPS); see http://www.mailabuse.org.
  - Message relay from a specified server or domain name to another server. There is also an anti-relay feature to block unauthorized senders from using the appliance to relay spam messages.

- Virus scanning of FTP exchanges for infected items.
- Virus scanning of HTTP web browsing, blocking infected content. You can also block Java, ActiveX and scripting.
- Virus scanning of POP3 e-mail messages, checking for infected items.
- Separate scanning for inbound and outbound traffic, allowing you to configure different scanning options for each direction.
- Separate automatic updating schedules for the appliance's McAfee virus definition (.DAT) files and McAfee scanning engine, ensuring up-to-date virus scanning at all times.
- Virus detection within common compressed file formats.
- Flexible scan actions that allow you to clean, delete, block or quarantine (isolate) infected items.
- Separate quarantine storage, allowing you to inspect the following types of quarantined e-mail messages:
  - Inbound messages containing infected items.
  - Outbound messages containing infected items.
  - Inbound messages containing banned content.
  - Outbound messages containing banned content.
- Notification upon detection of an infected item, using a variety of configurable alerting methods, such as e-mail messaging, XML logging, SNMP reporting and ePolicy Orchestrator reporting; see the Configuration Guide.
- Advanced logging of scan activities and protocol streams, allowing you to view past performance and delivery information. You can also generate charts, reports and logs from the user interface.

- McAfee ePolicy Orchestrator support, allowing you to integrate the appliance with an ePolicy Orchestrator server to produce advanced statistical, historical, management and graphical reports for the information recorded by the appliance; see the Configuration Guide.
- A quick backup process, allowing you to store and restore your appliance's settings quickly over the network; see page 55.
- A quick restoration process, allowing you to restore the appliance's software in the unlikely event of a problem; page 57.

What doesn't it do?

The appliance has many features, but remember the following:

- It is *not* a firewall. You must use it within your organization, behind your existing firewall.
- It is *not* a mail server. You might need to configure your firewall, mail server, web cache and other equipment to route protocol traffic through the appliance; see page 48.
- It is *not* a mail transfer agent, and does not keep copies of the e-mail messages that pass through it, unless they are quarantined or deferred.
- It is *not* a general-purpose web server for storing web pages.
- It is *not* a general-purpose server for storing extra software and files. Do not install any software on the appliance or add any extra files to it unless specifically instructed by the appliance's documentation or your support representative.
- In proxy mode, it handles SMTP, FTP, HTTP and POP3 traffic only. Do *not* attempt to route other traffic through the appliance.

What comes with the appliance?

Ensure that you have all the items that accompany the appliance, checking the product's packaging for any hidden compartments. If any of the items are missing or damaged, please contact your supplier.

Hardware and software

- Three Cat 5 (Category 5) UTP network cables with RJ-45 connectors:
  - The two blue cables are straight-through (uncrossed).
  - The orange cable is crossed.

  "Installing the appliance" on page 28 describes how you use these cables with the appliance.
- Mounting kit, for installing the appliance into a 19" (inch) rack.
- WebShield e500 Appliance recovery CD.
- Various power cords for different countries.

> **IMPORTANT:** Ensure that you use the power cord that is suitable for the country of use. If a suitable cable is not included, contact your supplier. Do not connect the appliance to a power source until you have read "Power and safety information" on page 3.

User documentation

This guide is just one of the documents that we have included with the appliance, to help you use the product effectively. See the Release Notes for a description of the other documentation components.

Supplementary documentation

- Warranty information and mail-back card.
- McAfee PrimeSupport information.
- Additional literature, such as special offers and third-party licenses.

What additional items are required?

You can use the mounting kit to install the WebShield e500 Appliance into a 19" (inch) rack. To install it into an alternative location, you might need addition equipment to prepare that location and secure the appliance in place. Ensure that you follow all safety warnings at all times; see "Power and safety information" on page 3.

To configure and manage the appliance, you must have a computer connected either to the same network as the appliance or directly to the appliance; see Step 4 on page 29. You can then use the computer's web browser to access the appliance's user interface.

Configuration computer's requirements

The appliance's user interface is optimized for Microsoft Internet Explorer v4.0, v5.0, v5.5 or v6.0, and supports Netscape Navigator v4.7.

When you access the appliance, it checks that your web browser contains the correct components, and displays dialog boxes for any missing components.

Your web browser must have the following enabled:

- Secure Sockets Layer (SSL) v3.0 encryption
- JavaScript
- ActiveX (for Microsoft Internet Explorer)
- Plug-ins (for Netscape Navigator)

The user interface displays best with the following screen settings:

- 65,536 colors (256 colors minimum)
- 1152x864 resolution

Restoring or upgrading the appliance's software

In addition to general management of the appliance, you might also need to do the following:

- Restore the appliance's software to both of the appliance's drives, in the unlikely event of a problem.
- Upgrade the appliance's software with a WebShield e500 Appliance upgrade CD.

To perform these tasks, you must connect a keyboard and monitor directly to the appliance; see page 57 for more details.

Updating the appliance anti-virus definition (.DAT) files and scanning engine

The appliance's automatic updating feature keeps the .DAT file and scanning engine up-to-date, maintaining full anti-virus protection. This feature is configured through the appliance's user interface (using a web browser); see page 47. You can also initiate immediate updates at any time, using the same set of user interface pages.

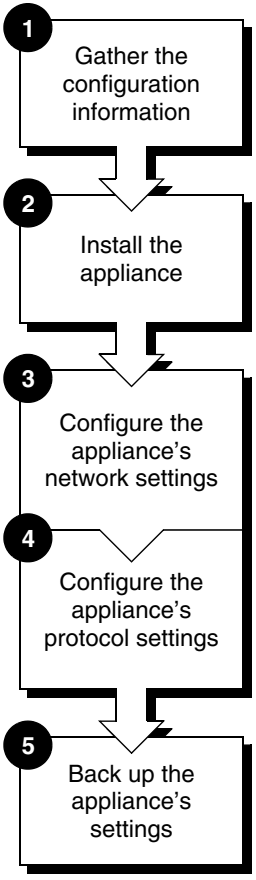
Installing Service Packs and HotFixes

You might receive Service Packs and HotFixes from your support representative, which contain improved software for the appliance. If this happens, you can install them through the appliance's user interface (using a web browser). Refer to the information that accompanies the Service Packs and HotFixes for information on installing them.

Getting started with the appliance

When you have decided how you want to use the appliance — see Chapter 1 of the Product Guide — you must perform the following actions to integrate the WebShield appliance with your current network:

1. Gather the required configuration information; see page 18.
2. Install the appliance in the required location, making the necessary connections; see page 28.
3. Configure the appliance's network settings; see page 32.
4. Configure the appliance's protocol settings; see page 40.
5. Back up your settings, so that you can reconfigure the appliance quickly if you need to restore its drives; see page 55.



When you have installed and configured the appliance, access its user interface to tailor the features that you require. For detailed information on configuring a feature in the user interface, view its Help topic by clicking the Help button; see page 54.

Who should install the appliance?

We strongly recommend that the Information Technology administrator responsible for your organization's e-mail system and Internet gateway installs and configures the appliance. The configuration process requires information for the protocols that you want to scan, and it must be configured correctly. Additionally, you might need to configure your other equipment to route traffic to the appliance, depending on which mode the appliance is using (proxy mode or transparency mode).

See page 18 for a summary of the required information.

Ports and connectors

The appliance's ports and connectors are shown on page vii (at the front of this guide). The installation steps on page 28 describe how to connect your equipment to the ports.

NOTE: We might change the physical appearance of the appliance at any time during manufacture. For this reason, the locations and types of the ports and connectors on your appliance might be different from those shown in this guide. If the changes are substantial, refer to the accompanying Release Notes for new information.

These ports and connectors are described below.

A Two hard disk drives

Both drives are 17.4GB "hot-pluggable" SCSI hard disk drives, managed in a RAID 1 (mirror) configuration. They mirror the appliance's operating system and data processing, ensuring seamless operation in the unlikely event of a problem with one of the drives (indicated by a red LED on the drive).
The drives are in caddies, allowing you to replace a faulty drive while the appliance is operational. The replacement drive is imaged automatically from the existing drive; see "One hard disk drive LED is red" on page 61.

B CD-ROM drive

The CD-ROM drive is used for restoring and upgrading the appliance's software, and must not be used at other times; see Step 4 on page 58.

C Control panel

The control panel on the bottom right-hand corner of the appliance contains LEDs that provide system information. There is also a reset button and power button:

Reset button
Restarts the appliance, simulating it being turned on and off.

Power button
Turns on the appliance, so that it is operational (the power LED is lit). If the power button is off, the appliance is in standby mode.

When the appliance is in standby mode, its network ports remain active but no protocols or data intended for the appliance can pass through it, maintaining your organization's anti-virus protection.

NOTE: If the power supply switch E (on the back of the appliance) is in the OFF position, the appliance does not receive any power.

Overheat LED
Lights when the appliance has overheated. This can be caused by poor airflow around the unit, or if room temperature exceeds normal operating conditions. Listen for the noise of the appliance's fan — in the center of the unit — to check that it is still working. If it does not appear to be working, turn off the appliance and contact your supplier.

Network activity LEDs
Flash when there is network activity on the network ports: NIC 1 is the LAN1 port, NIC 2 is the LAN2 port. If these LEDs flash when the power LED is off, the appliance is in standby mode.

CD-ROM drive activity LED
Flashes when the appliance is accessing the CD in the CD-ROM drive.

Power LED
Lights when the appliance is both switched on and operational.

D Power socket

Use the supplied power cord to connect the appliance to a power outlet.

IMPORTANT: Ensure that the power cord is suitable for the country of use. If it is not, contact your supplier.

E Power supply switch

Use this switch to turn on the appliance, so that it receives power from the connected power outlet.

NOTE: If the power supply switch is in the ON position but the power button (on the control panel C on the front of the appliance) is in the OFF position, the appliance is in standby mode.

F Keyboard port

Connect a keyboard to this port (colored purple) only if you are going to restore or upgrade the appliance's software; see Step 1 on page 58.

G Monitor port

Connect a monitor to this port only if you are going to restore or upgrade the appliance's software; see Step 2 on page 58.

H LAN1 port (NIC 1)

The LAN1 port is an RJ-45 10/100Mbps auto-sensing Ethernet network port, and is used to connect the appliance to your existing network. See Step 4 on page 29 for connection information.

The LAN1 port receives and transmits the following traffic:

- Inbound and outbound protocol traffic.
- Management and log data, including the communication from the remote web browser that you use to access the appliance's user interface. If you use ePolicy Orchestrator software with the appliance, its communication is also transmitted through this port.

The LAN1 port has a default IP address of 10.1.1.108 (subnet mask 255.255.255.0) to allow you to access the appliance initially across the network. When you configure the appliance, you can do the following:

- Add new IP addresses that are valid for your network.
- Modify or disable the default IP address.
- Delete the default IP address so that it cannot be used.

NOTE: For previous versions of the WebShield appliance, the LAN1 port was known as the *data port*, so you might see such references in existing documentation.

I LAN2 port (NIC 2)

The LAN2 port is an RJ-45 10/100Mbps auto-sensing Ethernet network port, and its operation depends on how you are using the appliance:

- **Proxy mode** — The LAN2 port can only be used for a direct local management connection. It *cannot* receive and transmit inbound and outbound protocol traffic.

  You might use this port if you cannot achieve a remote management connection through the LAN1 port, because of these reasons:

  - The LAN1 port's IP address belongs to a different subnet than your remote computer.
  - You have forgotten the LAN1 port's IP address that you set, and have disabled the default IP address of 10.1.1.108 for that port.

- **Transparency mode** — The LAN2 port is used (in conjunction with the LAN1 port) to connect the appliance to your existing network. It receives and transmits the same type of traffic as the LAN1 port.

See Step 4 on page 29 for connection information.

The LAN2 port has a default IP address of 10.1.2.108 (subnet mask 255.255.255.0). When you configure the appliance, you can do the following:

- Add new IP addresses that are valid for your network.
- Modify or disable the default IP address.
- Delete the default IP address so that it cannot be used.
- Disable the port so that it cannot be used.

IMPORTANT: If you are using transparency mode, do not disable the LAN2 port.

For previous versions of the WebShield appliance, the LAN2 port was known as the *management port*, so you might see such references in existing documentation.

Gathering the configuration information

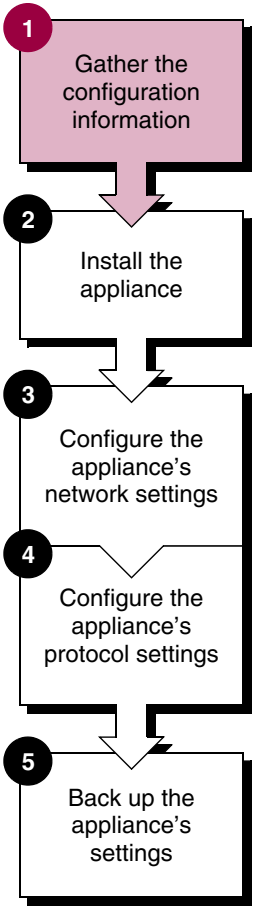
When you have decided how you want to use the appliance — see Chapter 1 of the Product Guide — you are ready to gather the required configuration information (step 1).

This section lists the information you must supply. We recommend that you gather the information before installation and configuration, so you can set up the appliance quickly.

We have provided spaces so that you can record the information on a printed copy of this section.

Chapter 11 of the Product Guide contains useful details about the configuration information that you can specify, and how it affects the operation of the appliance.

Step 2 — installing the appliance — is described on page 28.



Appliance host name

Supply the unique host name for the appliance:

Host name	

Domain

Supply the fully qualified domain or subdomain in which the appliance is located:

Domain name	

Examples: `myorg.com`, `network1.myorg.com`

Network addresses

Supply the TCP/IP network address information for the appliance:

	TCP/IP address
LAN1 port IP address and subnet mask	. . . . . .
LAN2 port IP address and subnet mask	. . . . . .
Local DNS server IP address	. . .
Default gateway or router IP address	. . .

NOTE: You can configure multiple IP addresses for the LAN1 and LAN2 ports.

For previous versions of the WebShield appliance, the LAN1 port was known as the *data port*, and the LAN2 port was known as the *management port*. Therefore, you might see such references in existing documentation.

Internal networks

Supply the domains or IP addresses for the internal networks (inside your organization) with which the appliance communicates. You can identify as many internal networks as you want (spaces for 10 networks are provided below):

NOTE: Remember to include the domain in which the appliance is located, unless you want that domain treated as an external network.

Network	Domain, or IP address and subnet mask
Example 1	myorg.com
Example 2	192 . 168 . 1 . 0 255 . 255 . 255 . 0
Example 3	*.myorg.com
1	. . .

	. . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . . . . .
7	. . . . . .
8	. . . . . .
9	. . . . . .
10	. . . . . .

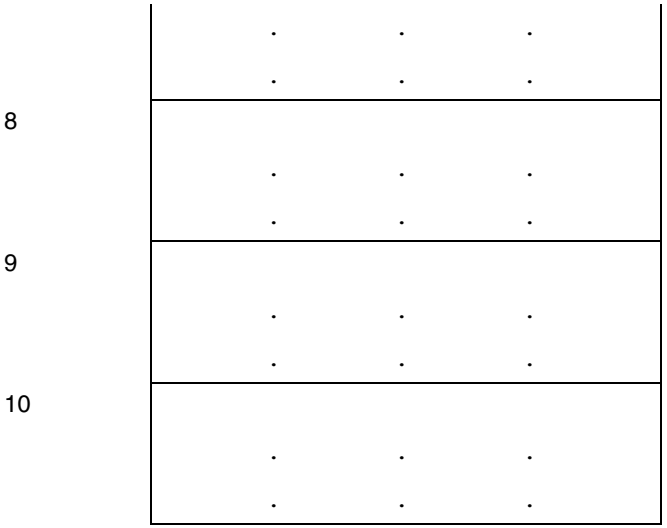
External networks

Supply the domains or IP addresses for the external networks (outside your organization) with which the appliance communicates. You can identify as many as you want (spaces for 10 networks are provided below):

IMPORTANT: We recommend that you keep the * domain entry in your external networks because it ensures that the appliance can proxy traffic for the Internet.

Ensure that you include the IP address of your firewall.

Network	Domain, or IP address and subnet mask
Example 1	testing.myorg.com
Example 2	sales.myorg.com
Example 3	*
1	
2	
3	
4	
5	
6	
7	



Proxy or transparency mode?

Decide which mode you want the appliance to use (it can use only one of these modes):

☐ Proxy mode (explicit proxy).

☐ Transparency mode (transparent proxy).

For more details about these modes, see the "Proxy or transparency?" section in the Product Guide.

IMPORTANT: Both modes are different so it is important that you understand and decide which mode you want to use *before* you install and configure the appliance.

Every network is different so the appliance must be configured with the correct information for your network to ensure correct operation. If you are unsure about of the information that you need to provide, consult your organization's networking expert.

Static routes and dynamic routing

When adding the appliance to your network, you need to ensure that all parts of your network can still communicate both internally and externally through the appliance. You can use static routes and dynamic routing at the appliance to configure this information so that the appliance knows how to reach various parts of your network:

- **Proxy mode** — There are circumstances where the appliance might need to use more than one gateway or router to communicate with the entire network. Specify these additional gateways and routers as static routes.
- **Transparency mode** — You might need to specify routing information for some of the internal and external communications through the appliance. Specify this routing information as static routes. Additionally, the appliance supports the RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) routing protocols, so you can use dynamic routing to gather the routing information from your network, if the network uses these protocols.

For each static route, supply the IP address and subnet mask to identify the network, and supply the IP address of the gateway or router used to reach that network. You can configure as many static routes as you want (spaces for 4 routes are provided below):

Route	Network IP address and subnet mask		Gateway or router IP address
Example	192 . 168 . 40 . 0 255 . 255 . 255 . 0	➡	192 . 168 . 50 . 3
1	. . . . . .	➡	. . .
2	. . . . . .	➡	. . .
3	. . . . . .	➡	. . .
4	. . . . . .	➡	. . .

If you want to use dynamic routing to obtain the routing information, check the following box:

☐ Enable dynamic routing.

Protocols

Check the boxes for the proxies that you want to enable, and the virus scanning that you want to enforce. Supply the ports on which your network transmits the protocols' traffic, if they are different from the defaults (provided in parentheses):

	Enable proxy	Scan inbound	Scan outbound	Port
E-mail (SMTP)	☐	☐	☐	(25)
File transfer (FTP)	☐	☐	☐	(21)
Web browsing (HTTP)	☐	☐	☐	(80)
Mail download (POP3)	☐	☐		(110)

NOTE: The appliance scans mail download (POP3) traffic without distinguishing its direction (inbound or outbound); see "Mail download (POP3)" on page 27. For this reason, there is just one checkbox.

Scanning profile

Check one of the following boxes to identify the expected usage profile:

☐ High constant SMTP, some HTTP, minimal FTP.

☐ Moderate constant SMTP, constant HTTP, minimal FTP.

☐ Very variable SMTP, constant HTTP, minimal FTP.

☐ User-selected values — The appliance uses the relevant settings in the protocols' configuration pages (in the user interface), allowing you to specify the configuration settings that you want.

NOTE: The usage profiles do not mention the mail download (POP3) protocol because it is typically used less frequently than the other protocols. However, as with the other proxies, the exact configuration settings for each protocol is available for modification on the protocol configuration pages (in the user interface) so that further adjustments can be made as required.

The following sections describe the additional required information for setting up the various protocols: "E-mail (SMTP)" on page 25, "File transfer (FTP)" on page 26 and "Mail download (POP3)" on page 27.

E-mail (SMTP)

Check the boxes for the required delivery methods:

☐ Locally configured domains; see below.

☐ DNS.

The appliance uses the DNS server that you specify when supplying the TCP/IP network address information; see "Network addresses" on page 19.

☐ Fallback relays; see page 26.

Locally configured domains

Supply the following information for the mail relays. You can create as many relays as you want (spaces for 15 relays are provided below). Identify the most common relays first because the appliance tries the relays in order:

Relay	E-mail domain		Fully-qualified hosts (mail servers)
Example 1	*myorg.com*	➡	*mail.uk.myorg.com*
Example 2	*myorg.co.uk*	➡	*mail1.us.myorg.com mail2.us.myorg.com*
Example 3	**.myorg2.com*	➡	*mail2.us.myorg.com*
1		➡	
2		➡	
3		➡	
4		➡	
5		➡	
6		➡	
7		➡	
8		➡	
9		➡	
10		➡	
11		➡	
12		➡	
13		➡	
14		➡	
15		➡	

Fallback relays

Supply the following information for the fallback relays. You can create as many relays as you want (spaces for 15 relays are provided below). Identify the most common relays first because the appliance tries the relays in order:

Relay	E-mail domain		Fully-qualified hosts
Example 1	*myorg.org*	→	*mail.externalorg1.com mail.externalorg2.com*
Example 2	*	→	*outmail.myorg.com*
1		→	
2		→	
3		→	
4		→	
5		→	
6		→	
7		→	
8		→	
9		→	
10		→	
11		→	
12		→	
13		→	
14		→	
15		→	

File transfer (FTP)

If you want to block 8-bit ASCII transfers over FTP, check the following box:

☐ Block 8-bit data transfer in ASCII mode.

NOTE: Some file transfer utilities use the 8-bit ASCII mode by default, so you must remember to change your utilities to binary mode, if the appliance is blocking the 8-bit ASCII mode.

For more information about FTP, refer to the Product Guide.

Mail download (POP3)

Generic proxy

When a generic proxy connection is made through the appliance, the appliance separates the user name, host name and port number with hash (#) and colon (:) delimiter characters:

```
user#host:port
```

To use different delimiter characters, supply them here:

user ☐ host ☐ port

❑ **NOTE:** As you configure the appliance with a port number for generic connections, your POP3 clients (software) do not need to specify that port number every time they make a generic POP3 connection through the appliance.

Dedicated proxy

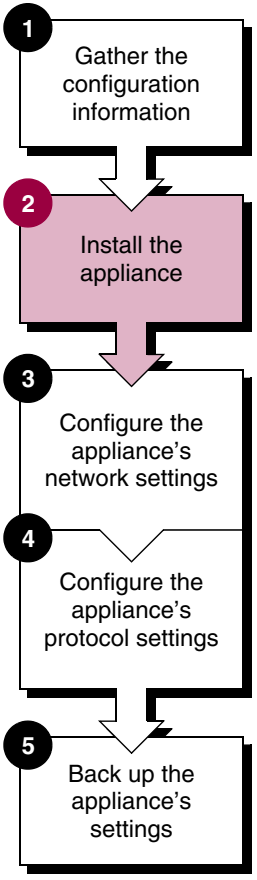
When a user makes a dedicated proxy connection through the appliance, the appliance uses a specified port to reach the POP3 server.

You can allow connections to as many servers as you want (spaces for 10 servers are provided below). Supply a unique port number and domain name for each server:

Server	Port	POP3 server domain name
Example	*1024*	*pop3server.externalorg.com*
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

For more information about POP3, refer to the Product Guide.

Installing the appliance



When you have gathered the required configuration information (see page 18), you are ready to install the appliance in the required location, making the necessary connections (step 2).

This chapter describes the installation steps. We recommend that you read them before performing the actions, to ensure that you know what is required.

See page 11 for a list of additional required items.

Step 3 — configuring the appliance's network settings — is described on page 32.

For details on the appliance's ports and connectors, see page 14.

To install the WebShield e500 Appliance:

1. Read the safety warnings in "Power and safety information" on page 3 and ensure that you follow them at all times.
2. Remove the WebShield e500 Appliance from any protective packaging and place it on a flat surface.
3. If you are going to install the appliance in a specific place, such as a 19" (inch) rack, perform the following steps ensuring that you follow all safety warnings; see "Power and safety information" on page 3:

    a. Prepare the intended location.

    You can use the mounting kit to install the WebShield e500 Appliance into a 19" (inch) rack. Follow the instructions on page viii (at the front of this guide).

    Ensure that you allow for adequate ventilation and access to the appliance's ports and connectors when you put it in place.

    b. Put the appliance in its intended location.

    Ensure that the appliance is secured firmly in place, so that it cannot fall.

4. Using the supplied network cables, connect the appliance to your network. The ports and cables that you use depend on how you are going to use the appliance:

   - **Proxy mode**

     LAN1 port: Using one of the supplied blue network cables — or an equivalent Cat 5 Ethernet cable — connect the appliance's LAN1 port (see H on page 16) to your existing network (Figure 1-2). The cable is a straight-through (uncrossed) cable, so you can connect the appliance to a normal uncrossed (MDI) RJ-45 port on your network equipment.

     This connection also allows you to manage the appliance from a remote computer, across the network.

     LAN2 port: In proxy mode, the appliance's LAN2 port becomes a dedicated management port. If you intend to manage the appliance locally, use the supplied orange network cable — or an equivalent crossover Cat 5 Ethernet cable — to connect the LAN2 port (see I on page 17) to your local computer's network card (Figure 1-2).

     You need only make this connection if you intend to manage the appliance locally.

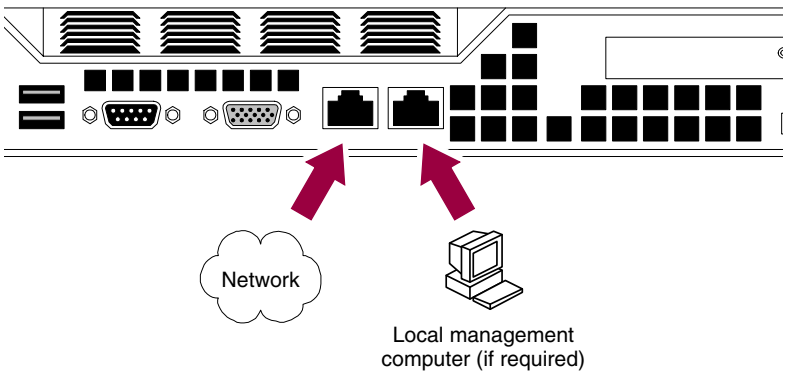


Figure 1-2. Connecting your appliance (proxy mode)

- **Transparency mode**

  LAN1 and LAN2 ports: Using both of the supplied blue network cables — or equivalent Cat 5 Ethernet cables — connect the appliance's LAN1 port (see H on page 16) and LAN2 port (see I on page 17) to your existing network (Figure 1-3) so that the appliance is inserted into the data stream. The cables are straight-through (uncrossed) cables, so you can connect the appliance to a normal uncrossed (MDI) RJ-45 ports on your network equipment.

  NOTE: In transparency mode, the appliance must be connected to two different subnets.

  The appliance must be used *inside* your firewall. For example, if your network is connected to the Internet through a hub and a firewall, you could put the appliance between the hub and firewall (connecting the hub to the LAN1 port and the firewall to the LAN2 port).

  In transparency mode, you can manage the appliance from a remote computer, across the network. However, you cannot obtain a local management connection through the LAN2 port (a method available with proxy mode) because that port is required for receiving and transmitting traffic.

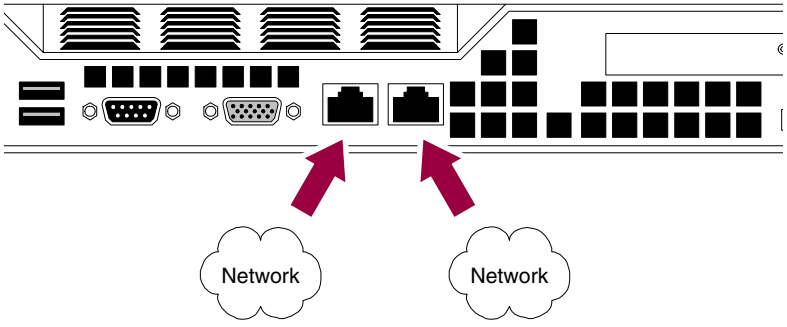


Figure 1-3. Connecting your appliance (transparency mode)

5. Use the supplied power cord to connect the appliance's power socket (see D on page 15) to a working power outlet.

IMPORTANT: Ensure that the power cord is suitable for the country of use. If it is not, contact your supplier.

The appliance's software is pre-installed so do not put a CD in the appliance's CD-ROM drive unless instructed to do so.

---

6. Turn on the appliance by pushing both the power supply switch and the power button to their ON positions (Figure 1-4).

   The power supply switch is on the back of the unit (see E on page 16). The power button is on the control panel on the front of the unit (see C on page 15).

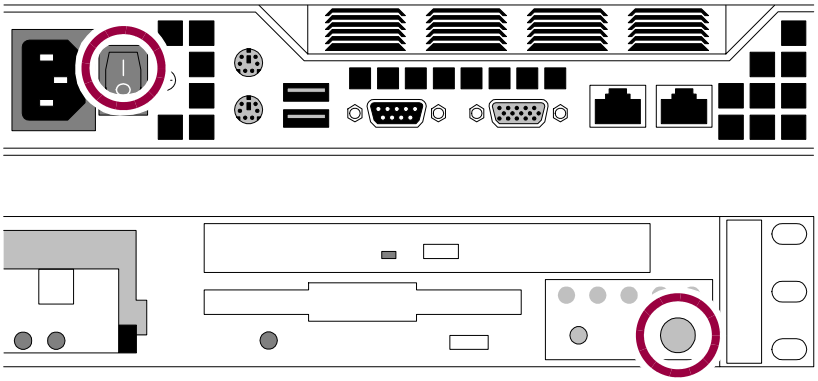
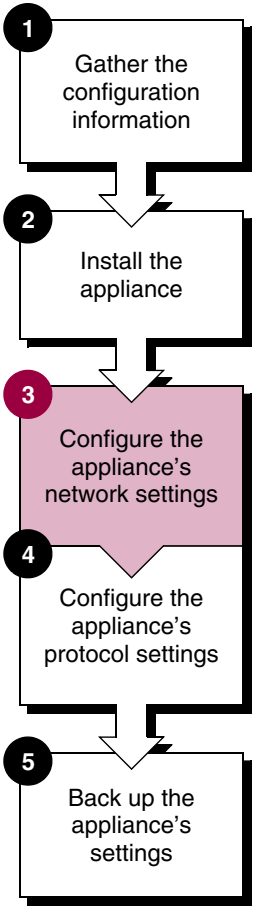


Figure 1-4. Turning on the appliance

The appliance performs its startup sequence and is ready for use after about two minutes. You can now configure the appliance's network settings; continue with page 32.

Configuring the network settings



When you have installed the appliance in the required location and made the necessary connections (see page 28), you are ready to configure the appliance's network settings (step 3).

This section describes the steps for configuring the network settings. We recommend that you read them before performing the actions, to ensure that you know what is required.

If you have already gathered the required configuration information (see page 18), you can configure the appliance more quickly.

To restore or upgrade the appliance's software, see page 57.

If you have previously created a set of configuration files from which you want to restore the appliance's settings, see "Restoring your settings" on page 56.

Step 4 — configuring the appliance's protocol settings — is described on page 40.

For details on the appliance's default settings, refer to Appendix A of the Product Guide.

To configure the appliance's network settings:

1. Open the web browser on the computer that you want to use to manage the appliance.
2. In the address field — where you can type a Uniform Resource Locator (URL) to open a web site — enter the following address:

   `https://<IP address>`

> **NOTE:** Ensure that you type `https`, not `http`.

The `<IP address>` that you use depends on how you are connected to the appliance:

- Remotely (across the network), through the LAN1 port — Use the LAN1 port IP address that you have configured for the appliance (it is `10.1.1.108` by default).
- Remotely (across the network), through the LAN2 port (available for transparency mode only) — Use the LAN2 port IP address that you have configured for the appliance (it is `10.1.2.108` by default).
- Locally, directly connected to the LAN2 port (available for proxy mode only) — Use the LAN2 port IP address that you have configured for the appliance (it is `10.1.2.108` by default).

NOTE: If you are using the appliance in transparency mode, use the IP address for the port and subnet to which your management computer is connected.

All management connections use Secure Sockets Layer (SSL) encryption, so they are secure. The SSL connection closes when you terminate the management session by clicking **Log off**. To maintain security during long management sessions, the SSL connection also closes after 15 minutes of inactivity.

When you configure new IP addresses for the LAN1 or LAN2 ports (Step 16 on page 36), the appliance *adds* the new address to the ports; it does not replace the default IP addresses. If you are using the appliance in proxy mode, the LAN2 port's IP address is a separate address, used solely for that port (it cannot be seen by the LAN1 port), that you can disable. You can use the LAN2 port for direct management access if you are unable to access the LAN1 port.

You must ensure that the web browser on the management computer (the computer you are using to manage the appliance) does not have the appliance configured as its proxy. If it is, the management connection does not work.

Additionally, if you have a proxy between the management computer and the appliance, the proxy must be configured with the appliance as its handoff host.

---

3. When the web browser finds the appliance, a Security Alert message might appear asking you to accept the appliance's security certificate. Click **Yes** to accept the certificate.

   TIP: The security alert message can appear at the start of each browser session. To stop this happening, you can view and install the certificate so that it is accepted automatically. To do this in Internet Explorer, click **View Certificate** in the Security Alert message, then click **Install Certificate** on the dialog box that appears.

   If you have just turned on the appliance, you must allow about two minutes for the startup sequence to finish or else the web browser might not find the appliance on the first attempt. If this happens, retry the URL. If you still cannot access the "Log on" page, see page 63.

   The appliance's "Log on" page appears. The appliance checks the web browser to ensure that it is supported and contains the required code to run the appliance's interface. For this reason, some security alerts and download dialog boxes might appear. Complete the dialog boxes as required.

   NOTE: The appliance's user interface needs the Java 2 Runtime Environment. If your web browser needs to install this, be aware that it is 5–14MB in size (depending on the components required by your browser) and can take a long time to install if you have a slow remote link to the appliance.

4. In **Language**, select the language in which you want to view the appliance's interface.

   This does not affect the language in which the appliance operates; see Step 14 on page 36.

5. If you chose English for the language, select the locale. This allows you to use a non-English character set when using the interface.

6. Click **Log on**.

   The Enter Network Password dialog box appears, asking you to supply your user name and password. The user name is `e500` and the default password is `e500changeme`. If you recently restored the appliance's software without maintaining the previous settings, the password reverts to the default password.

7. Type the user name and password, then click **OK**.

   The appliance's user interface appears, showing the System Configuration page.

   If you have configured the appliance before, the System Status page appears with a navigation bar on the left. To display the System Configuration page, select **System Configuration** in the navigation bar. For details on the user interface, see "Using the appliance" on page 53. For details on configuring a particular page, view the Help topic for that page by clicking the Help button.

   > **NOTE:** If you have a configuration file taken from an earlier version of the appliance, you can use the Restore Configuration panel to restore those settings to the appliance; see "Restoring your settings" on page 56.

8. In the **Appliance name** text box, type a unique host name for the appliance of no more than 15 characters (see "Appliance host name" on page 18).
9. In the **DNS server** text box, type the IP address of the local DNS server.
10. In the **Domain name** text box, type the domain or subdomain in which the appliance is located, such as `myorg.com` (see "Domain" on page 18).
11. In the **DNS server** text box, type the IP address of the local DNS server (see "Network addresses" on page 19).
12. If the appliance communicates with the network through a default gateway or router (firewall), type the gateway or router's IP address in the **Default gateway** text box (see "Network addresses" on page 19).

    There are circumstances where the appliance might need to use more than one gateway or router to communicate with the entire network. If this is required, you can specify these additional gateways and routers as static routes; see Step 22 on page 38.

13. To use the appliance in transparency mode, select **Enable Transparency**. Otherwise, leave the checkbox clear to use the appliance in proxy mode (see "Proxy or transparency mode?" on page 22).

14. In **System Language**, select the language in which you want the appliance to operate.

    This affects the reports and messages generated by the appliance, excluding any text strings that you can specify or modify through the interface. This is separate from the language used for viewing the interface (chosen when logging on to the appliance, see Step 4 on page 34).

15. If the LAN IP Addresses panel is not shown, click **LAN IP Addresses** to display the panel.

    This panel lists the IP addresses configured for the LAN1 and LAN2 ports.

16. Use the **Add** buttons under the LAN1 and LAN2 lists to specify new IP addresses for those ports (see "Network addresses" on page 19).

    You can specify multiple IP addresses for each port. The appliance adds them to the ports when you apply your changes (Step 27 on page 39). The new IP addresses do not overwrite the existing IP addresses. If you no longer want to use an IP address, you can either:

    - Modify or disable the IP address — select it from the list then click **Modify**. To disable it, select **Disable network address**.
    - Delete the IP address — select it from the list then click **Delete**.

    NOTE: We recommend that you access the appliance using your new IP addresses (after initial configuration) *before* removing the default IP addresses, to ensure that the new IP addresses work.

    If you are using the appliance in proxy mode, the LAN2 port becomes a dedicated management port, allowing you to make a direct local management connection.

17. To prevent any direct management connections to the appliance, you can disable the LAN2 port. To do this, select **Disable** under the LAN2 list.

> **IMPORTANT:** If you are using transparency mode, do not disable the LAN2 port.

The appliance uses two lists (Inside Networks and Outside Networks) to determine whether the traffic passing through it has comes from an internal or external source.

> **TIP:** If you have specific internal subdomains that you want to be treated as external networks, such as `testing.myorg.com`, you can use the Inside Networks and Outside Networks as follows:
>
> Inside networks:
>
> ```
> *.myorg.com
> ```
>
> Outside networks:
>
> ```
> testing.myorg.com
>
> *
> ```

18. Click **Inside Networks** to display the Inside Networks panel.
19. Use this panel to specify the domains or IP subnets for the internal networks within your organization (inside the firewall) that you want the appliance to protect (see "Internal networks" on page 19). You can specify as many networks as you want.

> **NOTE:** If you want the appliance to protect the domain in which the appliance is located (specified in Step 10 on page 35), you must add this domain to the Inside Networks list.

To add a network, click **Add**, then specify either its domain or its IP address and subnet mask in the Add dialog box that appears. Click **OK** to add it to the Inside Networks list.

20. Click **Outside Networks** to display the Outside Networks panel.

    This panel shows the networks configured as being external to the appliance. By default, the appliance uses the * wildcard symbol in its Outside Networks list to identify that all networks (other than those specified in the Inside Networks list) are external networks.

    IMPORTANT: We recommend that you keep the * domain entry in your external networks because it ensures that the appliance can proxy traffic for the Internet.

    Ensure that you include the IP address of your firewall.

    ---

21. Use this panel to specify the domains or IP subnets for the external networks outside your organization (outside the firewall). You can specify as many networks as you want (see "External networks" on page 21).

    To add a network, click **Add**, then specify either its domain or its IP address and subnet mask in the Add dialog box that appears. Click **OK** to add it to the Outside Networks list.

22. If you need to specify some static routes for various parts of your network so that the appliance know how to reach them (see "Static routes and dynamic routing" on page 23), click **Static Routes** and specify those routes in the Static Routes panel.

23. If you are using the appliance in transparency mode and want to use dynamic routing, click **Dynamic Routes** then select **Enable Dynamic Routing**.

    Dynamic routing is a system that allows your network equipment (including the appliance) to listen for the routing information that is broadcasted by the routers on your network. Remember that the appliance only supports the RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) routing protocols.

24. Click **Time and Password Settings** to display the Time and Password Settings panel.

25. Change the **Time zone**, **Date** and **Time** values to reflect the current date and time, then click **Set now**. The time is in 24-hour format.

    The appliance changes its date and time. These values are used when time-stamping the traffic that passes through the appliance, and when logging and alerting.

26. To change the password, type the new password in the **Password** text box, then retype it in the **Confirm** text box. Click **Set now**.

    IMPORTANT: For security reasons, we strongly recommend that you change the default password now (when configuring the appliance for the first time).

27. Click **Apply all changes**.

    The web browser sends your changes to the appliance. The user interface asks you to restart the appliance's software because you have made IP configuration changes.

28. Click **Restart now**.

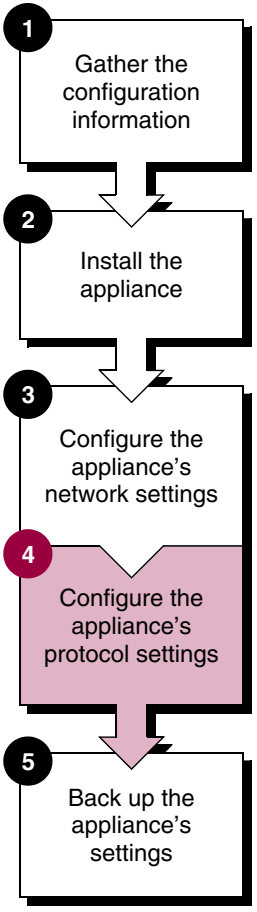
    The appliance restarts its software and is ready for use after about two minutes.

    The user interface displays a new URL hotlink that you can use to re-access the user interface with the new IP address.

29. When the appliance has restarted, click the URL hotlink or use one of the other IP addresses that you have configured for the port through which you are managing the appliance. If you were using the LAN2 port but chose to disable its IP address (Step 17 on page 37), access the LAN1 port across the network.

    When you have logged on, the System Status page appears with a navigation bar on the left. You can now configure the appliance's protocol settings; continue with "Configuring the protocol settings" on page 40.

Configuring the protocol settings



When you have configured the appliance's network settings (see page 32), you are ready to configure the appliance's protocol settings (step 4).

This section describes the steps for configuring the protocol settings. We recommend that you read them before performing the actions, to ensure that you know what is required.

If you have already gathered the required configuration information (see page 18), you can configure the appliance more quickly.

Step 5 — backing up the appliance's settings — is described on page 55.

Tasks

This section is divided into the following tasks that you must perform in order:

1. Configuring the appliance's protocols; see page 41.
2. Configuring the automatic updating feature, so that the appliance keeps its virus definition (.DAT) file and scanning engine up-to-date, maintaining full anti-virus protection; see page 47.
3. If necessary, configure your firewall, mail server, web cache and other equipment to route protocol traffic through the appliance; see page 48.
4. Testing your configuration, to ensure that it scans inbound and outbound traffic correctly for infections; see page 50.

Configuring the appliance's protocols

The WebShield e500 Appliance provides proxies for the SMTP, FTP, HTTP and POP3 protocols. It divides its resources between the proxies, virus scanning each protocol's inbound and outbound traffic (POP3 traffic directions are not distinguished) by default. For details on the proxies and protocols, see "Ports and connectors" on page 14.

To configure which protocols are enabled and virus scanned, and select the appropriate usage profile:

1. To disable the proxies for any of the protocols — to prevent the protocol's traffic passing through the appliance — deselect the appropriate checkboxes in the **Protocols enabled** section of the System Configuration page.

   NOTE: In transparency mode, this does not prevent traffic passing through the appliance.

2. To disable inbound or outbound virus scanning for any of the enabled protocols, select the appropriate **Configuration** page in the navigation bar (E-mail Configuration, File Transfer Configuration, Web Browsing Configuration or Mail Download Configuration), then deselect **Scan inbound traffic** or **Scan outbound traffic** as required (**Scan POP3 traffic** is used on the Mail Download Configuration page).

   WARNING: Do not disable virus scanning for any enabled protocol *unless* you are scanning its traffic at another point in your network. Allowing unscanned traffic to enter and leave your organization leaves you open to virus infection.

   Ensure that you have configured your other network equipment to route the protocols through the appliance (if necessary), so nothing can bypass the appliance; see page 48.

3. In the navigation bar, select **System Profiles**.

4. Select the most appropriate usage profile (see "Scanning profile" on page 24).

   The usage profiles do not mention the mail download (POP3) protocol because it uses much less bandwidth than the other protocols. If you have enabled scanning for the POP3 protocol, it is scanned regardless of which profile you choose.

   You can adjust any of the usage values (including the POP3 levels) in the Configuration pages for the protocols. If you do this, the appliance automatically selects **User-selected values from the 'Configuration' pages of each protocol** in the System Profiles page.

5. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

Configuring the ports used for the protocols

The appliance uses the following default ports for the protocols:

- E-mail (SMTP): 25
- File transfer (FTP): 21
- Web browsing (HTTP): 80
- Mail download (POP3): 110

If your organization's network uses different ports for the protocols, you must adjust the appliance's port numbers accordingly.

To change the port used for a protocol:

1. Select the protocol's **Configuration** page in the navigation bar.
2. In the **Port on which to listen...** text box, type the required port number (see "Protocols" on page 24).
3. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

Configuring the e-mail (SMTP) delivery methods

If the e-mail protocol is enabled (the default setting), you must configure the delivery methods that it uses.

This section only provides the information necessary to set up the e-mail delivery methods, so that the appliance can start scanning and delivering its traffic. There are many pages of features associated with this protocol; for details on configuring those pages, view their Help topics by clicking Help buttons; see page 54.

To configure the e-mail delivery methods:

1. In the navigation bar, select **E-mail Delivery**.
2. In the Methods Used panel, select the required delivery methods (see "E-mail (SMTP)" on page 25).
3. If you selected the **Local domains** delivery method, click **Local Domains**, and specify the mail relays in the panel that appears. You can specify as many mail relays as you want (see "Locally configured domains" on page 25).

   The mail relays route e-mail messages destined for specific domains (such as myorg.com) to their relevant mail servers (such as mail1.myorg.com). To add a mail relay, click **Add**, then specify the e-mail domain and host (mail server) in the Add dialog box that appears. Click **OK** to add it to the Local Domains list.

TIP: The appliance tries the mail relays in order. If one of the relays is successful for a message, the others are not attempted for that message. Therefore, use the **Move up** and **Move down** buttons to position the relays in the order that you want them. Put the most frequently used relays at the top of the list.

---

4. If you selected the **Fallback relays** delivery method, click **Fallback Relays** and specify the fallback relays in the panel that appears. You can specify as many fallback relays as you want (see "Fallback relays" on page 26).

   The fallback relays route e-mail messages that cannot be delivered using the other delivery methods. To add a fallback relay, click **Add**, then specify the e-mail domain and host (mail server) in the Add dialog box that appears. Click **OK** to add it to the Fallback Relays list.

   TIP: You can create one mail relay to route messages from all domains, by using the * wildcard symbol for the domain. If the wildcard entry is positioned beneath other entries in the Fallback Relays list, the appliance tries the other entries before attempting the wildcard entry.

   The Fallback Relays list can contain relays for local hosts (mail servers). This allows you the flexibility of having local domains tried *after* a DNS server lookup, to route undeliverable messages into the organization.

   The appliance tries the mail relays in order. If one of the relays is successful for a message, the others are not attempted for that message. Therefore, use the **Move up** and **Move down** buttons to position the relays in the order that you want them. Put the most frequently used relays at the top of the list.

   ---

5. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

Configuring whether 8-bit data transfers are allowed

The file transfer protocol (FTP) allows data to be passed between computers in two modes: binary and 8-bit ASCII (American Standard Code for Information Interchange). Binary is consistent across computer platforms, so its data can be scanned effectively.

NOTE: The appliance blocks the 8-bit ASCII transfer mode by default, because its data can contain different characters codes and formatting (depending on the computer systems in use), allowing viruses to be concealed easily.

If the file transfer protocol is enabled (the default setting), you can enable 8-bit data transfers.

To enable 8-bit data transfers:

1. In the navigation bar, select **File Transfer Configuration**.
2. Deselect **Block 8-bit data transfer in ASCII mode** (see "File transfer (FTP)" on page 26).
3. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

   NOTE: Some file transfer utilities use the 8-bit ASCII mode by default, so you must remember to change your utilities to binary mode.

Configuring the mail download (POP3) proxies

If the mail download protocol is enabled (the default setting), you can configure the delimiter characters (for generic proxy connections) and port numbers (for dedicated proxy connections).

When a user makes a generic proxy connection through the appliance, the appliance separates the user name, host name and port number with hash (#) and colon (:) delimiter characters by default:

```
user#host:port
```

To change the delimiter characters for generic POP3 proxy connections:

1. In the navigation bar, select **Mail Download Configuration**.
2. Specify the new delimiter characters that you want to use (see "Generic proxy" on page 27).
3. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

To specify the ports used for dedicated POP3 proxy connections:

1. In the Mail Download Configuration page, specify the port numbers and POP3 servers in the Dedicated Proxy Connections list. You can specify as many servers as you want, but their associated port numbers must be unique (see "Dedicated proxy" on page 27).

   To add a POP3 server, click **Add**, then specify the unique port number (typically between 1024–32767) and server domain name (such as pop3server.externalorg.com) in the Add dialog box that appears. Click **OK** to add it to the Dedicated Proxy Connections list.
2. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

Configuring the automatic updating feature

The automatic updating feature keeps the virus definition (.DAT) file and scanning engine up-to-date, maintaining full anti-virus protection.

IMPORTANT: When the appliance scans for viruses (according to your settings), it uses the virus scanning engine and current .DAT file to search for and remove the viruses. Many new viruses are discovered daily, so McAfee creates new definition files to provide protection from these viruses. Additionally, new versions of the virus scan engine are created occasionally.

To configure the automatic updating feature:

1. In the navigation bar, select **Anti-Virus Automatic Updating**.
2. In the FTP Download Site panel, specify the location from which the .DAT file and scanning engine are copied. The appliance obtains the .DAT file and scanning engine from the Network Associates FTP server (ftp.nai.com) by default.

   To use a different FTP server, change the following text boxes:

   - **Server name**
   - **Path to .DAT/engine files**
   - **Server user name** (if required)
   - **Password** (if required)

   If your connection must travel through a proxy server, provide information about that server in the following text boxes:

   - **Proxy server**
   - **Proxy port number**
   - **Proxy user name** (if required)
   - **Proxy password** (if required)

   For detailed information on configuring this page, view the Help topic by clicking the Help button.
3. Click **FTP Update Schedule**, and select the days and times (in 24-hour format) that you want the appliance to update its .DAT file and scanning engine.
4. Click **Apply all changes**.

   The web browser sends your changes to the appliance.

Configuring your other equipment

This section provides an overview of the changes that you might need to make to your other equipment, to fully integrate the appliance into your existing network. The changes depend on whether you are using the appliance in proxy mode or transparency mode:

- **Proxy mode** (explicit proxy) — You must configure your other network equipment to route the protocols through the appliance, so nothing can bypass the appliance. This includes configuring all your internal clients (such as HTTP, FTP and POP3 software) to use the appliance as a proxy server. In particular, ensure that your web clients' HTTP, FTP and Gopher settings are configured to use the HTTP port number. See "Routing protocols through the appliance," below.
- **Transparency mode** (transparent proxy) — By definition, transparency mode allows you to slot the appliance into you network without requiring much reconfiguration of your other equipment. However, you will still need to configure your SMTP e-mail system to pass e-mail traffic through the appliance. See "Modifying DNS server records" on page 49.

IMPORTANT: During the day-to-day use of your e-mail system, you might need to take the mail server offline to perform configuration changes or other maintenance tasks. Be aware that if you leave the appliance running, it will still accept and scan incoming e-mail messages but will be unable to pass them on (unless your e-mail setup includes a backup mail server). If the appliance is allowed to fill up with messages, it will run out of space. To avoid this problem, disable the SMTP proxy at the appliance when the mail server is offline. Your firewall should then return incoming messages as undeliverable.

Routing protocols through the appliance

Consult the documentation that accompanies your other equipment for detailed information on configuring the required options. When you have finished configuring the equipment, you can perform versions of the test on page 50 to ensure that your mail setup is correct. The appliance uses the following default ports for the protocols:

- E-mail (SMTP): 25
- File transfer (FTP): 21
- Web browsing (HTTP): 80
- Mail download (POP3): 110

If you have configured the appliance to use different ports for the protocols, you must adjust your other equipment to use those ports accordingly.

We also recommend that you configure your firewall to only send and receive internal traffic from the appliance (for the protocols proxied by the appliance).

Modifying DNS server records

Depending on your organization's network topology and the protocols that the appliance proxies, you might need to modify records for internal and external DNS servers; see the scenarios presented by Chapter 1 of the Product Guide.

In particular, if you have internal FTP, web or POP3 servers, you might need to create records for *external* DNS servers that match the internal FTP, web and POP3 servers to your firewall. For an internal web server, you also need to create records for the *internal* DNS server that match the web server's domain name to its IP address.

The records that you include at the DNS server (and their order) also determines whether you are implementing a fail-over, fail-closed or fail-safe configuration (see Chapter 1 of the Product Guide), so you must ensure that the records are listed correctly.

For details on modifying your DNS server software, refer to the information that accompanies it.

Testing your configuration

We recommend that you conduct the following tests (depending on the proxies you have enabled) to verify that the WebShield e500 Appliance is correctly integrated with your network:

- "Test 1: Verifying that e-mail messages (SMTP) are scanned and delivered correctly" on page 51.
- "Test 2: Verifying that file transfers (FTP) are scanned correctly" on page 52.
- "Test 3: Verifying that web browsing (HTTP) is scanned correctly" on page 52.
- "Test 4: Verifying that mail downloads (POP3) are scanned correctly" on page 53.

These tests use a special test file that has been developed by the European Institute of Computer Anti-virus Research (EICAR), a coalition of anti-virus vendors headquartered in Europe.

IMPORTANT: The EICAR test file *does not contain a virus* — it cannot spread or infect other files, or otherwise harm your system. Delete the file when you have finished testing your installation to avoid alarming other users.

Ensure that you disable the anti-virus software on the computer that you are using to create the EICAR test file, so that the anti-virus software does not remove the EICAR test file.

To create the EICAR test file:

1. Open a standard text editor, such as Microsoft Notepad.
2. Create a new text file, if necessary, and then type the following line:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
   ANTIVIRUS-TEST-FILE!$H+H*
   ```

   NOTE: The line shown above should appear as a single line in your text editor window.

3. Save the text file with the name EICAR.COM. The file size will be approximately 70 bytes.

Test 1: Verifying that e-mail messages (SMTP) are scanned and delivered correctly

You can test the appliance's SMTP virus scanning and delivery by sending the EICAR test file between internal and external (Internet) e-mail accounts.

To verify that SMTP virus scanning and delivery is working:

1. Log onto any computer in your network that has an e-mail account.
2. Create the EICAR test file.
3. Open your computer's e-mail program and create a new message with the following attributes: specify the intended recipient as an external e-mail address on the Internet to which you have access, and attach the EICAR file to the message.
4. Send the message.

   If your e-mail system is configured correctly, and the appliance has the default settings:

   - The mail server receives the outbound message from the internal computer, then delivers it to the appliance.
   - The appliance scans the message for viruses, and detects and removes the attached EICAR test file. It then returns the cleaned message to the internal e-mail account.
5. Check that the message is returned and does not contain the EICAR test file.
6. Access the external e-mail account on the Internet that you specified for the first message, and send a similar message to the internal e-mail account, attaching a new EICAR test file.

   If your e-mail system is configured correctly, and the appliance has the default settings, the appliance receives the reply message. It scans the message for viruses, and detects and removes the attached EICAR test file. It then returns the cleaned message to the external e-mail account.
7. Check that the message is returned and does not contain the EICAR test file.
8. Delete the EICAR test files that you created.

Test 2: Verifying that file transfers (FTP) are scanned correctly

You can test the appliance's FTP virus scanning by placing the EICAR test file on an FTP server, then trying to download it.

To verify that FTP virus scanning is working:

1. Log onto the FTP server.
2. Create the EICAR test file.
3. Log onto any computer in your network that has an FTP client (FTP software).
4. Open your computer's FTP client and connect to the FTP server.
5. Locate the EICAR test file and attempt to download it.

   If your FTP system is configured correctly, the appliance detects the EICAR test file and blocks the download.
6. Delete the EICAR test file that you created.

Test 3: Verifying that web browsing (HTTP) is scanned correctly

You can test the appliance's HTTP virus scanning by referencing the EICAR test file from a web page on a web server, then trying to download it.

To verify that HTTP virus scanning is working:

1. Log onto the web server.
2. Create the EICAR test file and reference it from a web page.
3. Log onto any computer in your network that has an HTTP client (web browser software).
4. Open your computer's HTTP client and access the web page with the EICAR test file.
5. Attempt to download the EICAR test file.

   If your HTTP system is configured correctly, the appliance detects the EICAR test file and blocks the download.
6. Delete the EICAR test file that you created.

Test 4: Verifying that mail downloads (POP3) are scanned correctly

You can test the appliance's POP3 virus scanning by sending the EICAR test file in a message to a POP3 e-mail account, then trying to download the message.

To verify that POP3 virus scanning is working:

1. Log onto any computer in your network that unscanned access to the POP3 server.
2. Create the EICAR test file and send it to a e-mail account on the POP3 server.
3. Log onto any computer in your network that has a POP3 client (POP3 mail download software).
4. Download the messages for the POP3 e-mail account that contains the message with the EICAR test file.

   If your POP3 system is configured correctly, the appliance detects the EICAR test file and removes it from the message.
5. Check that the message does not contain the EICAR test file.
6. Delete the EICAR test file that you created.

Using the appliance

The appliance's user interface (see page x at the front of this guide) has been designed for ease of use, to help you configure the appliance's settings quickly.

A Navigation bar

The navigation bar lists the features that can be configured (each has an arrow ▸ next to it). Click a feature to display its page of settings.

B Page

The page displays the settings for the feature that you selected in the navigation bar, allowing you to view and change those settings.

❑ **NOTE:** The changes that you make are not applied to the appliance until you click **Apply all changes**.

Each page contains the following buttons:

Product guide — Displays a PDF (Portable Document Format) version of the Product Guide.

Help — Opens the Help topic for the current page in a new browser window. The Help topics contain detailed information, including some tips on optimizing the appliance's features.

Cancel — Cancels the changes that you have made to the *current* page since you last applied changes to the appliance. If you move to another page, the web browser stores the page changes, so you must use **Cancel all changes** if you want to cancel the changes.

C Panel

Some pages have panels that containing more fields. Select the options in the page to view the panels.

D Control buttons

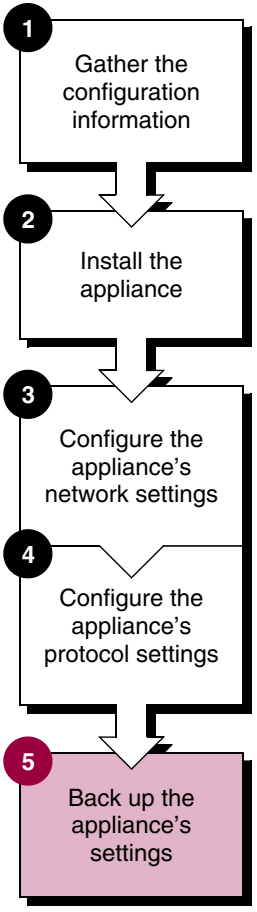
The user interface contains the following control buttons:

- **Log off** — Terminates the current management session. You return to the Log on page, and must log on again with your password to continue managing the appliance.
- **Apply all changes** — Applies the changes that you have made to the appliance.
- **Cancel all changes** — Cancels all the changes that you have made to *all* pages since you last applied changes to the appliance. If you made changes to multiple pages, all the changes are cancelled.

This guide does not provide detailed information for all of the user interface's pages. For that information, refer to the relevant Help topics.

Backing up and restoring your settings

When you have finished configuring the appliance's settings, we recommend that you back them up, so that you can quickly restore them should you need to restore the appliance's software in the unlikely event of a problem. Details on restoring the appliance's software are described in "Restoring and upgrading the appliance's software" on page 57.



Backing up your settings

To back up the appliance's settings to a set of configuration files:

1. Open the web browser on the computer on which you want to create the backup configuration files.
2. Access the appliance's user interface using the appropriate URL, and log on (see Step 2 on page 32 through Step 7 on page 35).
3. In the navigation bar, select **System Maintenance**.
4. Click **Save to file** next to "Save system settings."

   A File Download dialog box might appear for your browser, to verify that you want to download files from the appliance. If it does appear, click **OK**.

   The Save As dialog box appears.
5. Select the required location for the configuration files, and change the name of the .ZIP file as required. It is ws_cfg_backup.zip by default.
6. Click **Save**.

   The web browser creates the configuration files. If there are no problems, a confirmation dialog box appears.
7. Close the confirmation dialog box.

   You can now continue managing the appliance.

Restoring your settings

When you restore the appliance's settings with a configuration file, you must ensure that any other necessary changes are performed. For example, you can use the same configuration file for multiple appliances but those appliances cannot share IP addresses (IP addresses must be unique) so you would need to modify the IP addresses accordingly.

The appliance can use configuration files that were generated by an earlier version of the appliance. Therefore, if you generated such a file before upgrading your appliance, you can simply use the configuration file to restore your previous settings to the upgraded appliance.

To restore the appliance's settings from a set of configuration files:

1. Open the web browser on the computer that contains the backup configuration files, then access the appliance's user interface using the appropriate URL, and log on (see Step 2 on page 32 through Step 7 on page 35).

   If you are already accessing the appliance's user interface but the configuration files are on a different computer, transfer the files to the computer that you are using.

2. Depending on how you are configuring the appliance, do one of the following:

   - If you recently upgraded the appliance's software or you are configuring the appliance for the first time, the System Configuration page contains an extra Restore Configuration panel. Click **Restore Configuration** (on the System Configuration page) to access this panel.

     NOTE: The Restore Configuration panel is only available on the System Configuration panel when the appliance is first configured.

   - If you have configured the appliance before, select **System Maintenance** (in the navigation bar) to display the System Maintenance page. Focus on the **File** and **URL** text boxes next to "Restore System Settings."

3. In the **File** or **URL** text box, specify the full path or URL for the configuration files. Examples:

   ```
   c:\myfiles\ws_cfg_backup.zip
   ```

   ```
   http://www.myorg.com/myfiles/ws_cfg_backup.zip
   ```

   You can click **Browse** to locate the file.

4. Click **Restore now**.

   The web browser opens the configuration files, and sends the settings to the appliance. You can now continue managing the appliance.

Restoring and upgrading the appliance's software

If there is a problem with one of the appliance's hard disk drives, you can replace it with another drive (of the same specification) while the appliance is operational, and the appliance copies the image from the existing drive to the replacement drive; see page 61.

However, there might be circumstances where you need to restore the appliance's software to both of the appliance's drives. This is an unlikely situation but it can occur if you remove both drives from the appliance at the same time. The restoration process requires the WebShield e500 Appliance recovery CD.

You might also receive a WebShield e500 Appliance upgrade CD from your support representative, which contains improved software for the appliance. You upgrade the appliance's drives from this CD using a similar method to the restoration process.

❑ **NOTE:** You must connect to the appliance locally when restoring or upgrading its software. You cannot perform the restoration or upgrade remotely.

When restoring the appliance's software, the restoration process removes any additional software that you might have installed. If you are using ePolicy Orchestrator with the appliance, you must reinstall the ePolicy Orchestrator agent after the restoration process; see the Configuration Guide.

To restore or upgrade the appliance's software:

1. Connect a keyboard to the appliance's keyboard port (colored purple, see F on page 16).
2. Connect a monitor to the appliance's monitor port (see G on page 16).
3. Turn on the appliance, if it is off.
4. Insert the WebShield e500 Appliance recovery CD or upgrade CD into the appliance's CD-ROM drive (see B on page 14). The CD that you use depends on whether you are restoring or upgrading the software.
5. Push the reset button on the control panel on the front of the unit (see C on page 15).

   The appliance performs its startup sequence. It then reads the CD and displays a license agreement.

   NOTE: The following steps are correct for the WebShield e500 Appliance recovery CD. However, if the screen prompts are different for your CD, follow the screen prompts.

6. Read the license agreement carefully, then enter Y to accept it.

   If you do not accept the license agreement — entering N to reject it — you cannot use the software on the CD.

   The following options are presented:

   1: Perform a full installation removes all data from the appliance's hard disk drives and reinstalls the software.

   2: Install software on this CD reinstalls the software while attempting to preserve the areas containing the following items:

   - Configuration data
   - Log data
   - Quarantined e-mail messages
   - Deferred e-mail messages

   If the restoration process cannot preserve these areas, it re-creates them.

   3: Perform a software upgrade performs the appropriate software upgrades (if available) that are contained on the CD.

4: Automatic operation determines which of the three options above is suitable, and performs that option.

5: Perform a full installation and stop removes all data from the appliance's hard disk drives and reinstalls the software. After installation, the appliance ejects the CD but does not restart. You can then turn off the appliance.

6: Reset passwords to factory default returns the appliance's password to the default password `e500changeme`.

7: Do nothing and reboot leaves the appliance unchanged, and ejects the CD. You might want to choose this option if you inserted the CD by mistake, and do not want to restore or upgrade the appliance's software.

7. Enter the number for the required option.

   You are asked if you want to continue.

8. Enter `Y`.

   Unless you chose **7: Do nothing and reboot**, the restoration or upgrade process starts. A status screen shows the progress. Depending on the option that you chose, the process can take up to 30 minutes.

WARNING: Depending on the option that you choose, the appliance might revert to its default settings, losing the configuration settings that you have made.

When the restoration or upgrade process has finished, the appliance ejects the CD and restarts (unless you choose **5: Perform a full installation and stop**). When it has finished its startup sequence (after about two minutes), it is ready for use. Depending on the option that you chose, you might need to reconfigure the appliance's settings; see page 32.

NOTE: When you access the appliance and log on, be aware that the following changes might have occurred if you chose not to maintain the previous settings (or they could not be maintained):

- The password has reverted to the default password `e500changeme`.
- The LAN1 port has reverted to the default IP address 10.1.1.108.
- The LAN2 port is enabled and has reverted to the default IP address 10.1.2.108.

See Appendix A of the Product Guide for details on the appliance's default settings.

Troubleshooting

Hardware problems

This section contains solutions to problems that you can encounter when installing and running the appliance. See page 63 for solutions to user interface problems.

The appliance is not receiving power

Check the following:

- The appliance is connected properly to a working power outlet, using the supplied power cord.
- Both the power supply switch and the power button are in their ON positions; see Step 6 on page 31.

  The power supply switch is on the back of the unit (see E on page 16). The power button is on the control panel on the front of the unit (see C on page 15).

If the appliance is still not receiving power, check the power outlet by connecting it to other equipment. If the power outlet is working, there is a problem with the appliance or its power cord. Contact your supplier.

The appliance is not receiving traffic from my network

Check the following:

- The appliance is turned on and its software is running, indicated by the power LED being lit (on the control panel, see C on page 15) and the hard disk drive LEDs being off (see A on page 14).
- The network cables you are using are undamaged and connected properly to the appliance's ports and your existing network equipment. If you have not used the blue cables supplied with the appliance, ensure that the cables are Cat 5 (Category 5) UTP straight-through (uncrossed) network cables.
- You have connected the LAN2 port to your existing network equipment, if you are using the appliance in transparency mode.

If the appliance is still not receiving network traffic, check the network cables and the network ports on your exiting network equipment. If the cables and ports are working, there is a problem with the appliance. Contact your supplier.

One hard disk drive LED is red

The hard disk drive is faulty and must be replaced.

The drives are in caddies, allowing you to replace a faulty drive while the appliance is operational. The replacement drive is imaged automatically from the existing drive.

WARNING: When replacing the hard disk drives, ensure that you follow this information:

- Do not remove both drives from the appliance at any time. At least one drive must remain within the appliance at all times.
- Do not allow the appliance to be operational for more than a few minutes with one of the drives missing, because this disturbs the airflow and can result in the appliance overheating. Insert the replacement drive immediately.
- Only use drives that have exactly the same specification as the existing drives.
- When handling the drives, take care not to touch any static-sensitive components. Observe reasonable anti-static precautions, and do not insert your hand or any other object into the appliance's empty drive area.

To replace a faulty drive:

1. Push the faulty drive's release button, then pull its handle down (Figure 1-5). Pull the drive out of the drive area.

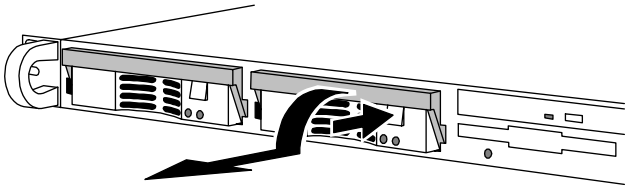


Figure 1-5. Removing the drive

2. Slide the replacement drive into the empty drive area, then push its handle up to lock the drive in place (Figure 1-6).

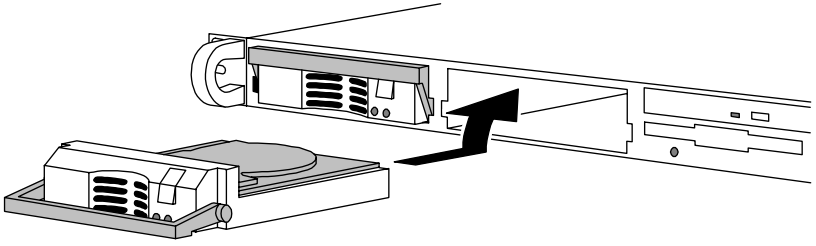


Figure 1-6. Inserting the drive

The appliance copies the image from the existing drive to the replacement drive. This can take 20–30 minutes. During this time, the replacement drive's green LED flashes.

Both hard disk drive LEDs are red

There is a problem with the appliance's drives. Use the WebShield e500 Appliance recovery CD to restore the appliance's software; see page 57. If this does not work, contact your supplier.

User interface problems

This section contains solutions to problems that you can encounter when trying to configure the appliance through its user interface.

I cannot access the “Log on” page

Check the following:

- The appliance is turned on and its software is running, indicated by the power LED being lit (on the control panel, see C on page 15) and the hard disk drive LEDs being off (see A on page 14).
- You have used `https` (not `http`) in the URL field of your web browser. Ensure that your browser supports Secure Sockets Layer (SSL) v3.0 encryption and that it is enabled.
- The management computer (the computer you are using to manage the appliance) does not have the appliance configured as its proxy. If you have a proxy between the management computer and the appliance, the proxy must be configured with the appliance as its handoff host.
- If you are remotely connected to the appliance (across the network) through the LAN1 port (see H on page 16), ensure that:
  - The computer that you are using has a working connection to your network, and that it can reach the same subnet to which the appliance is connected.
  - You have used the new IP address that you have configured for the LAN1 port, in the URL field of your web browser. If you have not disabled or deleted the default IP address `10.1.1.108`, try using that IP address (`https://10.1.1.108`).

    The appliance’s IP address must be suitable for the subnet to which the appliance is connected. If it is not, attempt to use the default IP address and, if that fails, try a direct management connection; see Step 4 on page 29.

    NOTE: You can only obtain a direct management connection through the LAN2 port if you are using the appliance in proxy mode *and* you have not disabled the LAN2 port (Step 17 on page 37).

  - The appliance has a working connection to your existing network, indicated by the NIC 1 network activity LED flashing (on the control panel, see C on page 15).

    If the LEDs are not flashing, ensure that the cable you are using is undamaged and connected properly to the appliance's LAN1 port and your existing network equipment. If you have not used the blue cable supplied with the appliance, ensure that the cable is a Cat 5 (Category 5) UTP straight-through (uncrossed) network cable.

- If the appliance is operating in proxy mode and you have a direct local management connection through its LAN2 port (see I on page 17), ensure that:

  - You have not disabled the LAN2 port. You must connect remotely to check this.

  - You have used the new IP address that you have configured for the LAN2 port (the default IP address is `10.1.2.108`), in the URL field of your web browser.

  - The appliance has a working connection to your computer, indicated by the NIC 2 network activity LED flashing (on the control panel, see C on page 15).

    If the LED is not flashing, ensure that the cable you are using is undamaged and connected properly to the appliance's LAN2 port and your computer's network port. If you have not used the orange cable supplied with the appliance, ensure that the cable is a Cat 5 (Category 5) UTP crossed network cable.

The "Log on" page appears but the Log on button is labelled "Initializing"

The appliance is checking your web browser for the components required by the user interface.

The appliance is optimized for Internet Explorer v4.0, v5.0, v5.5 or v6.0, and supports Netscape Navigator v4.7. If you are using a different web browser, you might be unable to access the user interface and configure the appliance.

The appliance's user interface needs the Java 2 Runtime Environment, so your browser might be installing this software. The Java 2 Runtime Environment is 5–14MB in size (depending on the components required by your browser) and it can take a long time to install if you have a slow remote link to the appliance.

My password does not work

If you recently restored the appliance's software without maintaining the previous settings, the password reverts to the default password `e500changeme`.

I have forgotten my password

You must use the WebShield e500 Appliance recovery CD to return the appliance's password to its default password `e500changeme`; see "Restoring and upgrading the appliance's software" on page 57. Use option **6: Reset passwords to factory default** during the restoration process.

Some of the user interface does not display properly

The appliance's user interface is optimized for Microsoft Internet Explorer v4.0, v5.0, v5.5 or v6.0, and supports Netscape Navigator v4.7. Check the accompanying release notes to see if there are known issues when using some web browsers on particular operating systems.

My clients (software) cannot communicate through the appliance

Check the following:

- The required proxies are enabled for the appliance (all supported protocols are enabled by default); see "Configuring the appliance's protocols" on page 41.
- The clients and other equipment are configured to route traffic to and from the appliance; see "Configuring your other equipment" on page 48.
- There are no network problems, and your equipment is connected correctly.

Web browsing does not work, or URL blocking is not enforced

The appliance must have access to a DNS server to verify web browsing (HTTP) requests and determine which URLs to block, if URL blocking is configured. Therefore, you must configure a DNS server in the System Configuration page; see Step 9 on page 35.

Installationshandbuch – Deutsch

Übersicht

In diesem Installationshandbuch finden Sie die zum Installieren oder Konfigurieren Ihres WebShield-Geräts erforderlichen Informationen. In folgenden Abschnitten finden Sie produktspezifische Informationen:

Copyright und Marken **Seite 2**

Informationen zu Stromversorgung und Sicherheit **Seite 3**

Infos zu WebShield e500 **Seite 5**

- Funktionen Seite 6
- Lieferumfang des WebShield e500 Seite 11

Erste Schritte mit dem Gerät **Seite 14**

- Wer das Gerät installieren sollte Seite 14
- Ports und Stecker Seite 15
- Zusammenfassen der Konfigurationsinformationen Seite 20

Installation des McAfee WebShield e500 **Seite 32**

Konfigurieren der Netzwerkeinstellungen **Seite 36**

Konfigurieren der Protokolleinstellungen **Seite 45**

- Konfigurieren der Protokolle des WebShield e500 Seite 46
- Konfigurieren der Funktion zum automatischen Aktualisieren Seite 52
- Konfigurieren weiterer Geräte Seite 53
- Testen Ihrer Konfiguration Seite 55

Verwenden des WebShield e250 **Seite 59**

- Sichern und Wiederherstellen der Einstellungen Seite 61
- Wiederherstellen und Aktualisieren der Gerätesoftware Seite 64

Fehlerbehebung **Seite 68**

- Hardwarefehler Seite 68
- Probleme mit der Benutzeroberfläche Seite 71

Copyright und Marken

COPYRIGHT
© 2001-2002 Networks Associates Technology, Inc. Alle Rechte vorbehalten. Kein Teil dieser Veröffentlichung darf ohne schriftliche Erlaubnis von Network Associates Technology, Inc., ihren Lieferanten oder zugehörigen Tochtergesellschaften in irgendeiner Form oder mit irgendwelchen Mitteln vervielfältigt, übertragen, transkribiert, in einem Informationsabrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Diese Genehmigung können Sie schriftlich bei der Rechtsabteilung von Network Associates unter der folgenden Adresse beantragen: 3965 Freedom Circle, Santa Clara, California 95054, USA, oder rufen Sie unter (+1) -972-308-9960 an.

MARKEN

Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, CyberCop, CyberCop (in Katakana), CyberMedia, CyberMedia UnInstaller, Design (stilisiertes N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, ISDN TEL/SCOPE, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctupus, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PC Medic 97, PCNotary, PGP, PGP (Pretty Good Privacy), Pretty Good Privacy, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, RingFence, Router PM, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SniffMaster, SniffMaster (in Hangul), SniffMaster (in Katakana), SniffNet, Stalker, SupportMagic, TIS, TMEG, TNV, TVD, TNS, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager sind eingetragene Marken von Network Associates, Inc. und der angeschlossenen Tochtergesellschaften in den USA und anderen Ländern. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind das alleinige Eigentum der jeweiligen Inhaber.

LIZENZVERTRAG

HINWEIS FÜR ALLE BENUTZER: Lesen Sie den entsprechenden rechtlichen Vertrag für die von Ihnen erworbene Lizenz sorgfältig durch. Er enthält die allgemeinen Bestimmungen und Bedingungen für die Verwendung der lizenzierten Software. Wenn Sie nicht wissen, welchen Lizenztyp Sie erworben haben, lesen Sie die Lieferdokumente und alle weiteren Lizenz- oder Bestellunterlagen, die der Software beiliegen oder die Sie als Teil des erworbenen Produkts erhalten haben (eine Broschüre, eine Datei auf der Produkt-CD oder eine Datei auf der Website, von der Sie das Softwarepaket heruntergeladen haben). SOLLTEN SIE NICHT MIT ALLEN BESTIMMUNGEN, DIE IM LIZENZVERTRAG ENTHALTEN SIND, EINVERSTANDEN SEIN, DÜRFEN SIE DIE SOFTWARE NICHT INSTALLIEREN. WENN DIESER FALL ZUTRIFFT, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES BEI NETWORK ASSOCIATES ODER AN DER STELLE ZURÜCKGEBEN, AN DER SIE ES ERWORBEN HABEN.

Informationen zu Stromversorgung und Sicherheit

WICHTIG: Um einen sicheren Betrieb des WebShield e500-Geräts zu gewährleisten, lesen Sie bitte folgende Informationen sorgfältig durch,*bevor* Sie das Gerät installieren.

Anforderungen zur Stromversorgung

- Prüfen Sie, ob das im Lieferumfang enthaltene Netzkabel für die Verwendung in Ihrem Land geeignet ist. Anderenfalls wenden Sie sich an Ihren Händler. Versuchen Sie auf keinen Fall, das Netzkabel zu verändern.
- Die Steckdose, an die Sie das Gerät anschließen, muß den gültigen elektrischen Standards des Landes, in dem sie das Gerät verwenden, entsprechen.
- Wenn Sie das Gerät an eine Steckdose oder andere Geräte anschließen, stellen Sie sicher, daß die Kabel so verlegt sind, daß keine Stolpergefahr für andere Personen besteht.

Verwenden des WebShield e500

- Öffnen Sie das Gehäuse des Geräts nicht. Es befinden sich keine Bauteile darin, zu denen der Benutzer Zugang benötigt.
- Das Gerät ist schwer. Wenn Sie es anheben oder an einen anderen Ort tragen möchten, versichern Sie sich, daß sie das Gerät sicher und fest in der Hand haben und es richtig tragen, um sich vor Verletzungen zu schützen und um das Gerät nicht zu beschädigen.
- Stellen Sie das Gerät nur auf einer ebenen und stabilen Unterlage ab, z. B. auf einem geeigneten Schreibtisch oder in einem 19-Zoll-Gestell. Vergewissern Sie sich, daß die Abstellfläche bzw. das Gestell stabil genug sind, um das Gewicht des Geräts auszuhalten und stellen Sie sicher, daß das Gerät nicht herunterfallen kann.
- Stellen Sie keine schweren Gegenstände auf dem Gerät ab.
- Die Netzwerk-Ports des WebShield e500 sind ausschließlich für die Verbindung mit einem RJ-45-Port geeignet. Verwenden Sie die Netzwerk-Ports nicht, um das Gerät an eine Telefonanlage anzuschließen, es sei denn, der Anschluß, den Sie verwenden, ist ausdrücklich für den Anschluß an ein 10/100-MBit/s-Ethernet-Netzwerk ausgelegt.
- Sollte ausnahmsweise ein Hardwarefehler am WebShield e250 auftreten, schalten Sie das Gerät aus und ziehen Sie den Netzstecker aus der Steckdose. Wenden Sie sich an Ihren Händler.

Betriebsbedingungen

- Versichern Sie sich, daß die Umgebungsbedingungen, unter denen das Gerät zum Einsatz kommen soll, für den Betrieb handelsüblicher Computer geeignet sind. Stellen Sie sicher, daß die Umgebung nicht feucht ist, und sorgen Sie für ausreichende Belüftung. Der Temperaturbereich für den Betrieb darf 10–40°C nicht über- bzw. unterschreiten und die Luftfeuchtigkeit muß zwischen 0% und 90% liegen. Werden diese Werte über- bzw. unterschritten, kann dies zum Versagen des Geräts führen.
- Sorgen Sie dafür, daß während des Betriebs immer ein Abstand von mindestens 25mm von der Rückseite des Geräts zur Wand bzw. zu anderen Geräten oder Möbeln eingehalten wird, um eine ausreichende Kühlung zu gewährleisten.
- Stellen Sie sicher, daß weder Flüssigkeiten noch Verunreinigungen oder fremde Gegenstände durch die Belüftungsschlitze oder das Belüftungsgitter in das Geräteinnere eindringen können.

Infos zu WebShield e500

Der WebShield e500 (Abbildung 2-1) ist ein spezieller Server zur Antiviren- und Inhaltsprüfung mit einer leistungsstarken neuen WebShield-Software. Der McAfee WebShield e500 kann mit Hilfe eines Web-Browsers vollständig konfiguriert und in nahezu jeder Netzwerktopologie eingesetzt werden. Er bietet eine Virenprüfung der folgenden Protokolle:

- Simple Mail Transfer Protocol (SMTP) E-Mail-Nachrichten
- File Transfer Protocol (FTP)-Austausch
- Hypertext Transfer Protocol (HTTP) für das Surfen im Internet
- Post Office Protocol Version 3 (POP3) Internet E-Mail-Nachrichten

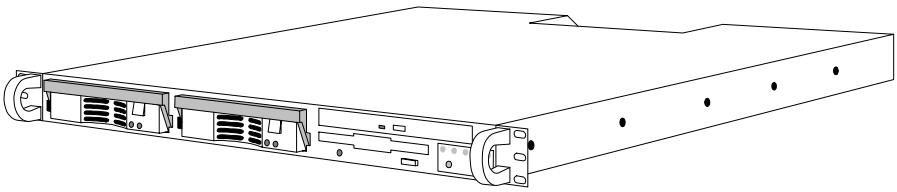


Abbildung 2-1. WebShield e500

Mit zusätzlichen Funktionen, wie beispielsweise Inhaltsüberwachung, Anti-Relay und Anti-Spam, bietet der WebShield e500 vollständigen Schutz für Ihr Internet Gateway. Es wird verhindert, daß unerwünschtes Material in Ihr Unternehmen gelangt oder dieses verläßt.

WebShield e500 verwendet seine Ressourcen gemeinsam mit den von der Anwendung verwendeten Protokollen. Eingehende und ausgehende Daten werden bei Bedarf überprüft. Die Anwendung kann infizierte E-Mail-Objekte, einschließlich komprimierter Dateien und Makros, erkennen, säubern, protokollieren und in den Quarantänebereich verschieben und dadurch verhindern, daß diese ihre vorgesehenen Empfänger erreichen. Außerdem können infizierte HTTP-, FTP- und POP3-Objekte blockiert werden.

Wenn Sie die Virenprüfung mit dem Gerät durchführen, bleibt Ihr Mailserver für Mailaktivitäten dediziert. Sie können auch mehrere WebShield e500 zusammen verwenden, um den Durchsatz beim Scannen zu erhöhen und eine Fehlertoleranz bereitzustellen.

Ausführliche Informationen über die verschiedenen Einsatzmöglichkeiten des Geräts sowie einige Beispieltopologien finden Sie in Kapitel 1 des Produkthandbuchs.

Funktionen

Transparenz – eine neue Funktion der Version 2.0

Benutzer früherer WebShield-Versionen sollten beachten, daß die Version 2.5 jetzt über eine zusätzliche Funktion verfügt, die sogenannte Transparenz-Funktion. Das bedeutet, das Gerät kann jetzt entweder im *Proxymodus* oder im *Transparenzmodus* betrieben werden:

- Der **Proxymodus** (expliziter Proxy) eignet sich für solche Netzwerke, bei denen es relativ einfach ist, die Netzwerkgeräte so zu konfigurieren, daß Protokollverkehr durch das Webshield-Gerät geleitet wird. Vor der Einführung des Tranzparenzmodus, arbeitete das Webshield-Gerät ausschließlich im Proxymodus.

  Im Proxymodus verarbeitet WebShield e500 nur den Datenverkehr der von ihm unterstützten Protokolle.

- Der **Transparenzmodus** (transparenter Proxy) ermöglicht die Einbindung des Webshield e500 in solche Netzwerke, bei denen das Konfigurieren der Netzwerkgeräte zu schwierig oder zu zeitaufwendig ist. In diesem Modus ist das Gerät transparent in das Netzwerk eingebunden: Empfang und Weiterleitung des gescannten Datenverkehrs erfolgen mittels statischer und dynamischer Routing-Informationen.

  > **HINWEIS:** Im Transparenzmodus muß das Gerät über die Ports LAN1 und LAN2 mit zwei getrennten Subnets verbunden sein.

  Das Gerät verarbeitet den gesamten IP-Datenverkehr zwischen zwei Subnets.

Ausführliche Informationen über diese Modi finden Sie im Abschnitt “Proxy oder Transparenz?“ im Produkthandbuch.

> **WICHTIG:** Beide Modi unterscheiden sich erheblich. *Bevor* Sie das Gerät installieren und konfigurieren, sollten Sie sich daher unbedingt näher mit der Funktionsweise beider Modi befassen und sich für denjenigen Modus entscheiden, der für Ihren Anwendungsfall geeignet ist.

Ausführliche Informationen zur Konfiguration des Webshield e500 mit der Konfigurationsdatei einer früheren Version des Geräts finden Sie unter “Wiederherstellen der Einstellungen“ auf Seite 62.

In diesem Abschnitt finden Sie außerdem eine Zusammenfassung einiger anderer Funktionen des Geräts.

Hardware

Der WebShield e500 verfügt über viele Funktionen, einschließlich der folgenden:

- 1U hoch 19" (Zoll) in einem Gestell installierbare Hardware.
- Duale Intel Pentium III 1 GHz-Prozessoren.
- 256MB PC133 SDRAM.
- Zwei RJ-45 10/100 MBit/s automatisch erfassende Ethernet-Netzwerk-Ports, die eine flexible Verbindung zu Ihrem vorhandenen Netzwerk und einer eigenen Verwaltungsoberfläche ermöglichen (nur im Proxymodus verfügbar).
- Zwei 17,4 GB während des Betriebs austauschbare SCSI-Festplattenlaufwerke in einer hardwarebasierten RAID 1-Konfiguration (Spiegelung). Dadurch wird für den unwahrscheinlichen Fall, daß bei einem der beiden Laufwerke Probleme auftreten, eine nahtlose Verarbeitung sichergestellt. Wenn Sie ein Ersatzlaufwerk einsetzen, wird das neue Laufwerk von dem RAID-Controller automatisch neu gespiegelt.

Weitere Informationen zu den Ports und Steckern des McAfee WebShield e500 finden Sie auf Seite 15.

Software

Die Software auf dem Gerät hat folgende Funktionen:

- Webverwaltung durch Secure Sockets Layer (SSL)-Verschlüsselung mittels eines Web-Browsers.
- Eine leicht konfigurierbare Benutzeroberfläche, mit der Sie das Gerät schnell einrichten können. Das Gerät erfordert danach minimalen Benutzereingriff und wird dadurch zu einer Konfigurieren-und-Vergessen-Lösung.
- Flexible Proxys, die selbst in komplexen Umgebungen einfach zu konfigurieren sind (siehe "Zusammenfassen der Konfigurationsinformationen" auf Seite 20).

- Scannen von SMTP-E-Mail-Nachrichten, Überprüfen auf infizierte Objekte und gesperrten Inhalt. Weitere SMTP-Funktionen umfassen:
  - Flexible Zustellungskonfiguration von SMTP-E-Mail, mit der Sie mehrere Zustellmethoden für E-Mail einrichten und eine Fehlertoleranz einführen können.
  - Flexible Inhaltsüberwachung von Nachrichten, wodurch Sie nach gesperrtem Inhalt suchen und bestimmte Anhangtypen blockieren können.
  - Blockieren von Spam (Abweisen unerwünschter E-Mail-Nachrichten) nach Empfänger, Absender oder Server.
  - Unterstützung von Schwarzen Listen in Echtzeit, die mögliche Quellen von Spam-Nachrichten identifizieren. Mit Hilfe dieser Listen kann das Gerät Spam-Nachrichten blockieren. Schwarze Listen werden von vielen Organisationen zur Verfügung gestellt, einschließlich des Mail Abuse Prevention System (MAPS, siehe http://www.mailabuse.org).
  - Nachrichten-Relay von einem bestimmten Server oder Domänennamen an einen anderen Server. Es steht auch eine Anti-Relay-Funktion zur Verfügung, um unbefugte Absender daran zu hindern, das Gerät als Relais für Spam-Nachrichten zu verwenden.
- Scannen von FTP-Austausch nach infizierten Objekten.
- Scannen beim Surfen im Internet (HTTP), Sperren infizierter Inhalte. Sie können außerdem Java, ActiveX und Scripting sperren.
- Virenprüfung von POP3-E-Mail-Nachrichten, Überprüfen auf infizierte Objekte.
- Getrenntes Scannen für eingehende und ausgehende Daten mit der Möglichkeit, für jede Richtung unterschiedliche Scan-Optionen zu konfigurieren.
- Getrennte, automatische Aktualisierungspläne für die McAfee-Virusdefinitionsdateien (DAT-Dateien) und das Scan-Modul von McAfee für das Gerät, wodurch die Virenprüfung jederzeit auf dem neuesten Stand ist.
- Virusentdeckung in üblichen komprimierten Dateiformaten.
- Flexible Scan-Aktionen, mit denen Sie infizierte Objekte säubern, löschen, blockieren oder in den Quarantänebereich verschieben (isolieren) können.

- Getrennte Speicherung des Quarantänebereichs; ermöglicht eine Überprüfung der folgenden Typen von E-Mail-Nachrichten im Quarantänebereich:
  - Eingehende Nachrichten, die infizierte Objekte enthalten.
  - Ausgehende Nachrichten, die infizierte Objekte enthalten.
  - Eingehende Nachrichten, die gesperrte Inhalte enthalten.
  - Ausgehende Nachrichten, die gesperrte Inhalte enthalten.
- Benachrichtigung bei Entdecken eines infizierten Objekts durch eine Vielzahl konfigurierbarer Warnmeldungen, beispielsweise E-Mail-Meldungen, XML-Protokollierung, SNMP-Berichterstellung und ePolicy Orchestrator-Berichterstellung (siehe Konfigurationshandbuch).
- Erweiterte Protokollierung von Scan-Aktivitäten und Protokollströmen, mit der Sie Informationen zu vergangenen Nutzungen und Übermittlungsinformationen anzeigen können. Von der Benutzeroberfläche aus können Sie auch Diagramme, Berichte und Protokolle erstellen.
- Unterstützung von McAfee ePolicy Orchestrator, mit der Sie das Gerät in einen ePolicy Orchestrator-Server integrieren können, um erweiterte statistische, chronologische, administrative und graphische Berichte für die von der Anwendung aufgezeichneten Daten erstellen zu können (siehe Konfigurationshandbuch).
- Ein schneller Sicherungsvorgang, durch den Sie die Einstellungen des Geräts schnell über das Netzwerk speichern und wiederherstellen können (siehe Seite 61).
- Ein schneller Wiederherstellungsvorgang zum Wiederherstellen der Gerätesoftware für den unwahrscheinlichen Fall eines Problems; Seite 64.

Was nicht möglich ist

Das Gerät verfügt über viele Funktionen, doch bedenken Sie folgendes:

- Es ist *keine* Firewall. Sie müssen das Gerät in Ihrem Unternehmen verwenden, hinter Ihrer vorhandenen Firewall.
- Es ist *kein* Mailserver. Es kann u. U. erforderlich werden, Ihre Firewall, Mailserver, Web-Cache und weitere Geräte so zu konfigurieren, daß Protokollverkehr durch das Gerät geleitet wird (siehe Seite 53).
- Es ist *kein* Mailübertragungsagent und behält keine Kopien der E-Mail-Nachrichten, die das Gerät durchlaufen, es sei denn, diese werden in den Quarantänebereich verschoben oder zurückgestellt.
- Es ist *kein* vielseitiger Webserver zum Speichern von Webseiten.
- Es ist *kein* vielseitiger Server zum Speichern von zusätzlicher Software und Dateien. Installieren Sie keine Software auf dem Gerät oder fügen Sie keine zusätzlichen Dateien hinzu, es sei denn, Sie werden in der Dokumentation zu dem Gerät oder von Ihrem Support-Mitarbeiter ausdrücklich dazu aufgefordert.
- Das Gerät stellt nur Proxys für die Protokolle SMTP, FTP, HTTP und POP3 zur Verfügung. Sie dürfen *nicht* versuchen, anderen Datenverkehr durch das Gerät zu leiten.

Lieferumfang des WebShield e500

Vergewissern Sie sich, daß alle Teile vorhanden sind, die mit dem Gerät geliefert werden. Überprüfen Sie die Produktverpackung, um sicherzustellen, daß Sie kein Teil übersehen haben. Falls eines der Teile fehlt oder beschädigt ist, wenden Sie sich an Ihren Händler.

Hardware und Software

- Zwei UTP-Netzwerkkabel der Kategorie 5 mit RJ-45-Ports:
  - Die beiden blauen Kabel sind durchgehende (ungekreuzte) Kabel.
  - Das orangefarbene Kabel ist gekreuzt.

  "Installation des McAfee WebShield e500" auf Seite 32 beschreibt, wie die Kabel zusammen mit dem Gerät verwendet werden.
- Montagesatz zum Einbau des Geräts in ein 19-Zoll-Gestell.
- WebShield e500-Wiederherstellungs-CD.
- Verschiedene Netzkabel für unterschiedliche Länder.

> **WICHTIG:** Prüfen Sie, ob das verwendete Netzkabel für die Verwendung in Ihrem Land geeignet ist. Falls kein geeignetes Kabel mitgeliefert wurde, wenden Sie sich an Ihren Händler. Schließen Sie das Gerät nicht an eine Stromquelle an, bevor Sie die Informationen in "Informationen zu Stromversorgung und Sicherheit" auf Seite 3 gelesen haben.

Benutzerdokumentation

Dieses Handbuch ist nur eines der Dokumente, die dem Gerät beigelegt sind, damit Sie das Produkt wirksam verwenden können. In den Versionshinweisen finden Sie eine Beschreibung der weiteren Dokumentationskomponenten.

Zusätzliche Dokumentation

- Garantie-Informationen und Rücksendepostkarte.
- McAfee PrimeSupport-Informationen.
- Zusätzliche Literatur, wie beispielsweise Sonderangebote und Lizenzen anderer Hersteller.

Zusätzlich erforderliche Teile

Sie können den Montagesatz verwenden, um WebShield e500 in einem 19-Zoll-Gestell zu installieren. Um das Gerät an einem anderen Standort installieren zu können, benötigen Sie u. U. zusätzliche Ausrüstungsgegenstände, um den Standort vorzubereiten und das Gerät zu sichern. Stellen Sie sicher, daß Sie jederzeit alle Sicherheitshinweise beachten (siehe "Informationen zu Stromversorgung und Sicherheit" auf Seite 3).

Um das Gerät zu konfigurieren und zu verwalten, muß ein Computer entweder mit demselben Netzwerk wie das Gerät oder direkt mit dem Gerät verbunden sein (siehe Schritt 4 auf Seite 33). Mit dem Web-Browser des Computers können Sie dann auf die Benutzeroberfläche des Geräts zugreifen.

Voraussetzungen für den Konfigurationscomputer

Die Benutzeroberfläche des Geräts wurde für Internet Explorer v4.0, v5.0, v5.5 oder v6.0 optimiert und unterstützt Netscape Navigator v4.7.

Wenn Sie auf das Gerät zugreifen, prüft dieses, ob Ihr Web-Browser die richtigen Komponenten enthält, und zeigt für alle fehlenden Komponenten Dialogfelder an.

In Ihrem Web-Browser muß folgendes aktiviert sein:

- Secure Sockets Layer (SSL) v3.0-Verschlüsselung
- JavaScript
- ActiveX (für Microsoft Internet Explorer)
- Plug-Ins (für Netscape Navigator)

Die Benutzeroberfläche wird mit den folgenden Bildschirmeinstellungen am besten angezeigt:

- 65 536 Farben (mindestens 256 Farben)
- Auflösung 1152 x 864

Wiederherstellen oder Aktualisieren der Gerätesoftware

Zusätzlich zur allgemeinen Verwaltung des Geräts müssen Sie u. U. auch folgendes durchführen:

- Im unwahrscheinlichen Fall eines Problems die Gerätesoftware auf beiden Laufwerken des Geräts wiederherstellen.
- Aktualisieren Sie die Gerätesoftware mit einer WebShield e500-Aktualisierungs-CD.

Um diese Tasks durchführen zu können, müssen Sie eine Tastatur und einen Monitor direkt an das Gerät anschließen, weitere Informationen finden Sie auf Seite 64.

Aktualisieren der Virusdefinitionsdateien (DAT-Dateien) des Geräts und des Scan-Moduls

Durch die automatische Aktualisierungsfunktion werden die DAT-Datei und das Scan-Modul auf dem neuesten Stand gehalten, wodurch vollständiger Virenschutz gewährleistet wird. Diese Funktion wird mit einem Web-Browser über die Benutzeroberfläche des Geräts konfiguriert (siehe Seite 52). Sie können auch jederzeit sofortige Aktualisierungen starten, indem Sie dieselbe Benutzeroberfläche verwenden.

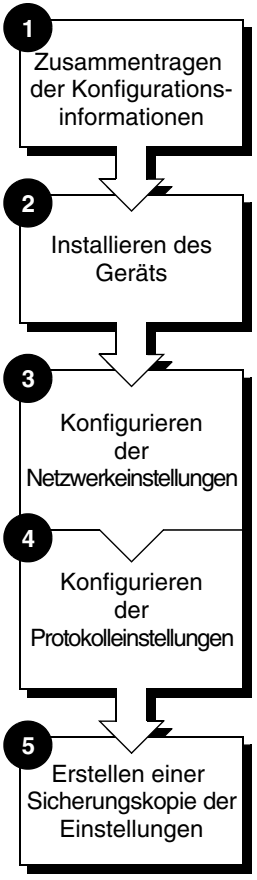
Installieren von Service Packs und HotFixes

U. U. erhalten Sie von Ihrem Support-Mitarbeiter Service Packs und HotFixes, die verbesserte Software für das Gerät enthalten. In diesem Fall können Sie diese mit einem Web-Browser über die Benutzeroberfläche des Geräts installieren. Genauere Informationen zu deren Installation finden Sie in den mit den Service Packs und HotFixes gelieferten Informationen.

Erste Schritte mit dem Gerät

Sobald Sie sich für eine Verwendungsweise des Gerät entschieden haben (siehe Kapitel 1 im Produkthandbuch), müssen Sie die folgenden Aktionen durchführen, um den WebShield e500 in Ihr aktuelles Netzwerk zu integrieren:

1. Sammeln von erforderlichen Konfigurationsdaten (siehe Seite 20).
2. Installieren des Geräts am erforderlichen Standort und Herstellen der nötigen Verbindungen (siehe Seite 32).
3. Konfigurieren der Netzwerkeinstellungen des Geräts (siehe Seite 36).
4. Konfigurieren der Protokolleinstellungen des Geräts (siehe Seite 45).
5. Erstellen einer Sicherungskopie Ihrer Einstellungen, so daß Sie das Gerät schnell neu konfigurieren können, falls Sie dessen Laufwerke wiederherstellen müssen (siehe Seite 61).



Sobald Sie das Gerät installiert und konfiguriert haben, greifen Sie auf dessen Benutzeroberfläche zu, um die benötigten Funktionen auf Ihre Bedürfnisse abzustimmen. Weitere Informationen zum Konfigurieren einer Funktion auf der Benutzeroberfläche erhalten Sie, indem Sie auf die Schaltfläche “Help“ (Hilfe) klicken und das entsprechende Hilfethema anzeigen (siehe Seite 59).

Wer das Gerät installieren sollte

Es wird dringend empfohlen, daß der IT-Administrator, der für das E-Mail-System und das Internet Gateway des Unternehmens verantwortlich ist, das Gerät installiert und konfiguriert. Für den Konfigurationsvorgang werden Daten für die Protokolle benötigt, die gescannt werden sollen, und die Konfiguration muß ordnungsgemäß ausgeführt werden. Außerdem kann es, abhängig vom Modus, in welchem Sie das Gerät betreiben (Proxymodus oder Transparenzmodus), erforderlich sein, die anderen Netzwerkgeräte so zu konfigurieren, daß sie die Protokolle durch das Gerät leiten.

Eine Zusammenfassung der erforderlichen Informationen finden Sie auf Seite 20.

Ports und Stecker

Die Ports und Stecker des Geräts sind auf Seite vii dargestellt (am Anfang dieses Handbuchs). Die Installationsschritte auf Seite 32 beschreiben, wie die Geräte an die Ports angeschlossen werden.

HINWEIS: U. U. wird das Erscheinungsbild des Geräts zu einem beliebigen Zeitpunkt während der Herstellung verändert. Aus diesem Grund können sich die Positionen und Arten der Ports und Stecker an Ihrem Gerät von denen unterscheiden, die in diesem Handbuch dargestellt sind. Falls die Änderungen wesentlich sind, finden Sie in den begleitenden Versionshinweisen neue Informationen.

Diese Ports und Stecker sind unten beschrieben.

A Zwei Festplattenlaufwerke

Beide Laufwerke sind 17,4 GB große, während des Betriebs austauschbare SCSI-Festplattenlaufwerke, die in einer hardwarebasierten RAID 1 -Konfiguration (Spiegelung) verwaltet werden. Auf den Festplatten wird das Betriebssystem und die Datenverarbeitung des Geräts gespiegelt, um im unwahrscheinlichen Fall eines Problems mit einem der beiden Laufwerke (angezeigt durch die rot leuchtende LED des Laufwerks) einen nahtlosen Betrieb sicherzustellen. Die Laufwerke sind in Caddies untergebracht, so daß Sie ein fehlerhaftes Laufwerk ersetzen können, während das Gerät in Betrieb ist. Das Ersatzlaufwerk wird automatisch von dem vorhandenen Laufwerk abgebildet (siehe “Eine LED des Festplattenlaufwerks leuchtet rot“ auf Seite 69).

B CD-ROM-Laufwerk

Das CD-ROM-Laufwerk wird zum Wiederherstellen und Aktualisieren der Gerätesoftware verwendet und darf sonst nicht verwendet werden (siehe Schritt 4 auf Seite 64).

C Bedienungsfeld

Das Bedienungsfeld in der rechten unteren Ecke des Geräts enthält die LEDs, die Systeminformationen bereitstellen. Außerdem sind eine Zurücksetzen-Taste und ein Ein-Schalter vorhanden.

Zurücksetzen-Taste
Startet das Gerät neu, wobei ein Aus- und Wiedereinschalten simuliert wird.

Ein-Schalter
Zum Einschalten des Geräts, so daß es betriebsbereit ist (die Strom-LED leuchtet). Falls die Strom-LED nicht leuchtet, befindet sich das Gerät im Bereitschaftsmodus (Standby-Modus).

Befindet sich das Gerät im Bereitschaftsmodus (Standby-Modus), bleiben die Netzwerk-Ports aktiv, doch es können keine Protokolle oder für das Gerät bestimmte Daten passieren, so daß der Virenschutz für Ihr Unternehmen erhalten bleibt.

❑ **HINWEIS:** Falls der Stromversorgungsschalter E (an der Rückseite des Geräts) sich in der AUS-Stellung befindet, bekommt das Gerät keinen Strom.

Überhitzungs-LED
Leuchtet auf, wenn das Gerät überhitzt. Dies kann durch mangelhafte Belüftung des Geräts verursacht werden, oder wenn die Raumtemperatur die normalen Betriebsbedingungen überschreitet. Hören Sie auf das Geräusch des Lüfters des Geräts (im Inneren des Geräts), um zu überprüfen, ob dieser noch arbeitet. Falls der Lüfter nicht mehr zu arbeiten scheint, schalten Sie das Gerät aus, und wenden Sie sich an Ihren Händler.

Netzwerkaktivitäts-LEDs
Blinken, wenn an den Netzwerk-Ports Netzwerkaktivitäten stattfinden. NIC 1 ist der LAN1-Port, NIC 2 ist der LAN2-Port. Ist die Strom-LED ausgeschaltet und diese LEDs blinken, befindet sich das Gerät im Bereitschaftsmodus (Standby-Modus).

CD-ROM-Laufwerkaktivitäts-LED
Blinkt, wenn das Gerät auf die CD im CD-ROM-Laufwerk zugreift.

Strom-LED
Leuchtet auf, wenn das Gerät eingeschaltet und betriebsbereit ist.

D Netzanschluß

Verwenden Sie das im Lieferumfang enthaltene Netzkabel, um das Gerät an eine Steckdose anzuschließen.

WICHTIG: Prüfen Sie, ob das im Lieferumfang enthaltene Netzkabel für die Verwendung in Ihrem Land geeignet ist. Anderenfalls wenden Sie sich an Ihren Händler.

E Stromversorgungsschalter

Schalten Sie das Gerät mit diesem Schalter ein, so daß es Strom von der Steckdose erhält, an die es angeschlossen ist.

HINWEIS: Falls der Stromversorgungsschalter sich in der EIN-Stellung befindet, doch der Ein-Schalter (im Bedienungsfeld C an der Vorderseite des Geräts) befindet sich in der AUS-Stellung, ist das Gerät im Bereitschaftsmodus (Standby-Modus).

F Tastatur-Port

Schließen Sie nur dann eine Tastatur an diesen Port an (violett markiert), wenn Sie die Gerätesoftware wiederherstellen oder aktualisieren möchten (siehe Schritt 1 auf Seite 64).

G Monitor-Port

Schließen Sie nur dann einen Monitor an diesen Port an, wenn Sie die Gerätesoftware wiederherstellen oder aktualisieren möchten (siehe Schritt 2 auf Seite 64).

H LAN1-Port (NIC 1)

Der LAN1-Port ist ein RJ-45 10/100 MBit/s automatisch erfassender Ethernet-Netzwerk-Port, über den das Gerät mit Ihrem vorhandenen Netzwerk verbunden wird. Weitere Verbindungsinformationen finden Sie unter Schritt 4 auf Seite 33.

Der LAN1-Port empfängt und überträgt folgende Daten:

- Ein- und ausgehenden Protokollverkehr.
- Verwaltungs- und Protokollierungsdaten, einschließlich der Kommunikation von dem Remote-Web-Browser, mit dem Sie auf die Benutzeroberfläche des Geräts zugreifen. Falls Sie ePolicy Orchestrator-Software auf dem Gerät verwenden, wird diese Kommunikation ebenfalls durch diesen Port übertragen.

Der LAN1-Port hat die standardmäßige IP-Adresse 10.1.1.108 (Subnet-Maske 255.255.255.0), um Ihnen zunächst über das Netzwerk Zugriff auf das Gerät zu ermöglichen. Wenn Sie das Gerät konfigurieren, können Sie folgendes tun:

- Neue (für Ihr Netzwerk gültige) IP-Adressen hinzufügen.
- Standard-IP-Adressen ändern oder deaktivieren.
- Löschen Sie die Standard-IP-Adresse, so daß sie nicht verwendet werden kann.

❑ **HINWEIS:** In früheren WebShield-Versionen wurde der LAN1-Port als *Daten-Port* bezeichnet. Daher ist es möglich, daß Sie in vorhandenen Dokumentationen Hinweise auf diesen Port finden.

I LAN2-Port (NIC 2)

Der LAN2-Port ist ein RJ-45 10/100 MBit/s automatisch erfassender Ethernet-Netzwerk-Port. Seine Funktionsweise hängt davon ab, wie das Gerät eingesetzt wird:

- **Proxymodus** – Der LAN2-Port kann nur für direkte lokale Verwaltungsverbindungen verwendet werden. Dieser Port *kann keine* eingehenden und ausgehenden Protokolldaten übertragen.

  Sie können diesen Port verwenden, falls Sie aus folgenden Gründen keine Remote-Verwaltungsverbindung über den Daten-Port herstellen können:

  - Die IP-Adresse des LAN1-Ports gehört zu einem anderen Subnet als Ihr Remote-Computer.
  - Sie haben die IP-Adresse für den LAN1-Port vergessen, die Sie eingestellt haben, und haben die standardmäßige IP-Adresse 10.1.1.108 für diesen Port deaktiviert.

- **Transparenzmodus** – Der LAN2-Port wird (gemeinsam mit dem LAN1-Port) verwendet, um das Gerät mit einem vorhandenen Netzwerk zu verbinden. Er empfängt und leitet denselben Datentyp weiter wie der LAN1-Port.

Weitere Verbindungsinformationen finden Sie unter Schritt 4 auf Seite 33.

Der LAN2-Port hat die Standard-IP-Adresse 10.1.2.108 (Subnet-Maske 255.255.255.0). Wenn Sie das Gerät konfigurieren, können Sie folgendes tun:

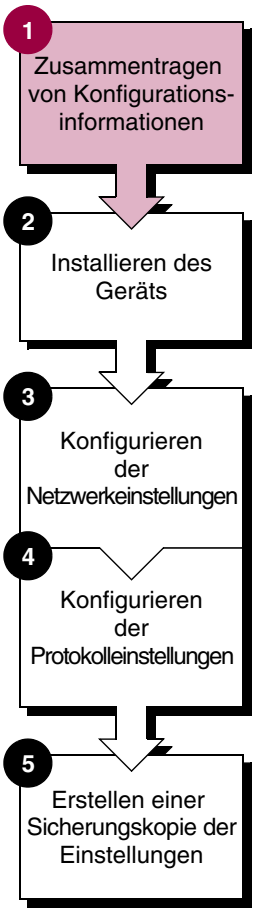
- Neue (für Ihr Netzwerk gültige) IP-Adressen hinzufügen.
- Standard-IP-Adressen ändern oder deaktivieren.
- Löschen Sie die Standard-IP-Adresse, so daß sie nicht verwendet werden kann.
- Deaktivieren Sie den Port, so daß er nicht verwendet werden kann.

WICHTIG: Deaktivieren Sie den LAN-Port **nicht**, wenn Sie den Transparenzmodus eingestellt haben.

In früheren WebShield-Versionen wurde der LAN2-Port als *Verwaltungs-Port* bezeichnet. Daher ist es möglich, daß Sie in vorhandenen Dokumentationen Hinweise auf diesen Port finden.

Zusammenfassen der Konfigurationsinformationen

Sobald Sie sich für eine Verwendungsweise für das Gerät entschieden haben (siehe Kapitel 1 im Produkthandbuch), können Sie die erforderlichen Konfigurationsinformationen zusammentragen (Schritt 1).



In diesem Abschnitt werden die Informationen aufgelistet, die Sie bereithalten müssen. Es wird empfohlen, diese Informationen vor der Installation und Konfiguration zu sammeln, so daß Sie das Gerät schnell einrichten können.

Es wurde Raum gelassen, damit Sie die Informationen auf einer gedruckten Ausgabe dieses Abschnitts aufzeichnen können.

In Kapitel 11 des Produkthandbuchs finden Sie nützliche Einzelheiten über die Konfigurationsinformationen, die von Ihnen festgelegt werden können, sowie darüber, wie sich diese Angaben auf die Funktionsweise des Geräts auswirken.

Schritt 2, Installieren des Geräts, wird auf Seite 32 beschrieben.

Hostname des Geräts

Geben Sie einen eindeutigen Hostnamen für das Gerät an:

Hostname _____

Domäne

Geben Sie die vollständig qualifizierte Domäne oder Subdomäne an, in der sich das Gerät befindet.

Domänenname _____

Beispiele: `meinefirma.com`, `netzwerk1.meinefirma.com`

Netzwerkadressen

Geben Sie die TCP/IP-Netzwerk-Adreßinformationen für das Gerät an:

	TCP/IP-Adresse
IP-Adresse des LAN1-Port und Subnet-Maske	. . . . . .
IP-Adresse des LAN2-Port und Subnet-Maske	. . . . . .
IP-Adresse des lokalen DNS-Servers	. . .
Standard-Gateway oder IP -Adresse des Routers	. . .

☐ **HINWEIS:** Sie können mehrere IP-Adressen für die Ports LAN1 und LAN2 konfigurieren.

In früheren WebShield-Versionen wurde der LAN1-Port als *Daten-Port* bezeichnet, und der LAN2-Port als *Verwaltungs-Port*. Daher ist es möglich, daß Sie in vorhandenen Dokumentationen Hinweise auf diese Ports finden.

Interne Netzwerke

Stellen Sie die Domänen oder IP-Adressen für die internen Netzwerke bereit (innerhalb Ihres Unternehmens), mit denen das Gerät kommuniziert. Sie können beliebig viele interne Netzwerke angeben (unten wurde Raum für zehn Netzwerke gelassen).

☐ **HINWEIS:** Schließen Sie die Domäne ein, in der sich das Gerät befindet, es sei denn, diese Domäne soll als externes Netzwerk behandelt werden.

Netzwerk	Domäne oder IP-Adresse und Subnet-Maske
Beispiel 1	meinefirma.com
Beispiel 2	192 . 168 . 1 . 0 255 . 255 . 255 . 0
Beispiel 3	*.meinefirma.com
1	. . .

	. . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . . . . .
7	. . . . . .
8	. . . . . .
9	. . . . . .
10	. . . . . .

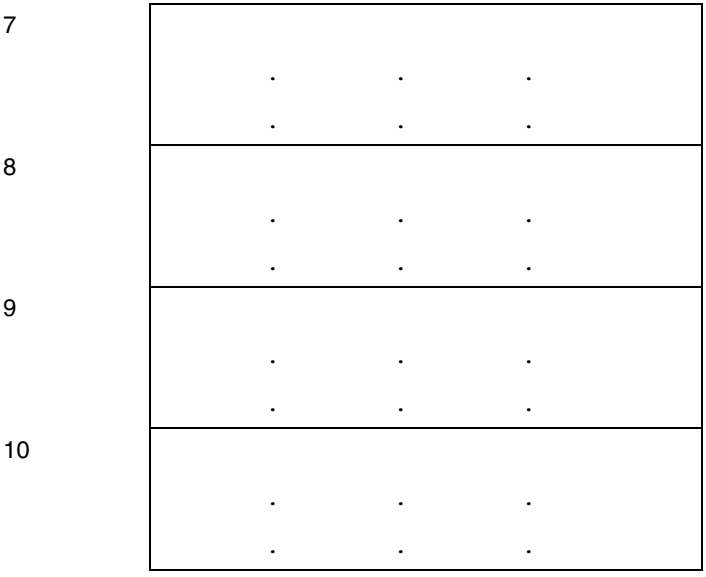
Externe Netzwerke

Stellen Sie die Domänen oder IP-Adressen für die externen Netzwerke bereit (außerhalb Ihres Unternehmens), mit denen das Gerät kommuniziert. Sie können beliebig viele externe Netzwerke angeben (unten wurde Raum für zehn Netzwerke gelassen).

WICHTIG: Es wird empfohlen, den * -Domäneneintrag in Ihren externen Netzwerken zu behalten, weil dadurch sichergestellt wird, daß das Gerät stellvertretend Datenverkehr für das Internet empfängt.

Vergessen Sie nicht, auch die IP-Adresse für Ihre Firewall anzugeben.

Netzwerk	Domäne oder IP-Adresse und Subnet-Maske
Beispiel 1	test.meinefirma.com
Beispiel 2	vertrieb.meinefirma.com
Beispiel 3	*
1	. . . . . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . . . . .



Proxy- oder Transparenzmodus?

Legen Sie den Betriebsmodus für das Gerät fest (es kann jeweils nur einer der beiden Modi verwendet werden):

☐ Proxymodus (expliziter Proxy).

☐ Transparenzmodus (transparenter Proxy).

Ausführliche Informationen über diese Modi finden Sie im Abschnitt “Proxy oder Transparenz?“ im Produkthandbuch.

WICHTIG: Beide Modi unterscheiden sich voneinander. *Bevor* Sie das Gerät installieren und konfigurieren, sollten Sie sich daher unbedingt näher mit der Funktionsweise beider Modi befassen und sich für denjenigen Modus entscheiden, der für Ihren Anwendungsfall geeignet ist.

Da jedes Netzwerk anders ist, muß das Gerät mit den richtigen Daten für Ihr Netzwerk konfiguriert werden, um einen fehlerfreien Betrieb zu gewährleisten. Wenn Sie nicht sicher sind, welche Daten Sie angeben müssen, wenden Sie sich an den Netzwerkspezialisten Ihrer Firma.

Statische Routen und dynamisches Routing

Wenn Sie das Gerät zu Ihrem Netzwerk hinzufügen, überprüfen Sie, ob sowohl die interne als auch die externe Kommunikation zwischen den Netzwerkkomponenten über das Gerät noch einwandfrei funktioniert. Sie können diese Daten sowohl mit statischen Routen als auch durch dynamisches Routing konfigurieren. Dies ist erforderlich, damit WebShield e500 Zugang zu den verschiedenen Komponenten des Netzwerks hat:

- **Proxymodus** – Unter bestimmten Umständen benötigt das Gerät eventuell mehr als ein Gateway oder mehrere Router, um mit dem gesamten Netzwerk kommunizieren zu können. Geben Sie diese zusätzlichen Gateways und Router als statische Routen an.
- **Transparenzmodus** – U. U. müssen Sie Routing-Informationen für einen Teil der internen und externen Kommunikation über das Gerät eingeben. Geben Sie diese Routing-Informationen als statische Routen ein. WebShield e500 unterstützt außerdem die Routing-Protokolle RIP (Routing Information Protocol) und OSPF (Open Shortest Path First). Daher können Sie diese Protokolle verwenden, um die benötigen Routing-Informationen von Ihrem Netzwerk zu bekommen – vorausgesetzt, das Netzwerk verwendet diese Protokolle.

Geben Sie zur Identifizierung des Netzwerks für jede statische Route die IP-Adresse und die Subnet-Maske an sowie die IP-Adresse des zur Verbindung mit diesem Netzwerk verwendeten Gateways oder Routers. Sie können beliebig viele statische Routen konfigurieren (unten wurde Raum für 4 Routen gelassen).

Route	IP-Adresse und Subnet-Maske des Netzwerks		IP-Adresse des Gateways bzw. Routers
Beispiel	192 . 168 . 40 . 0 255 . 255 . 255 . 0	→	192 . 168 . 50 . 3
1	. . . . . .	→	. . .
2	. . . . . .	→	. . .
3	. . . . . .	→	. . .
4	. . . . . .	→	. . .

Wenn Sie dynamisches Routing verwenden möchten, um die Routing-Informationen zu erhalten, aktivieren Sie das folgende Kontrollkästchen:

☐ Dynamisches Routing aktivieren

Protokolle

Aktivieren Sie die Kontrollkästchen für die Proxys, die aktiviert werden sollen, und für die Virenprüfung, die Sie erzwingen möchten. Stellen Sie die Ports bereit, über die Ihr Netzwerk die Daten des Protokolls überträgt, falls sie sich von den Standard-Ports unterscheiden (in Klammern angegeben):

	Proxy aktivieren	Eingehende scannen	Ausgehende scannen	Port
E-Mail (SMTP)	☐	☐	☐	(25)
Dateiübertragung (FTP)	☐	☐	☐	(21)
Surfen im Internet (HTTP)	☐	☐	☐	(80)
Mail-Download (POP3)	☐	☐		(110)

❑ **HINWEIS:** Das Gerät scannt Mail-Downloads (POP3), ohne die Richtung zu ermitteln (eingehend oder ausgehend, siehe "Mail-Download (POP3)" auf Seite 30). Aus diesem Grund gibt es nur ein Kontrollkästchen.

Scanning profile (Scan-Profil)

Aktivieren Sie eines der folgenden Kontrollkästchen, um das erwartete Verwendungsprofil zu identifizieren:

➡ "High constant SMTP, some HTTP, minimal FTP" (SMTP konstant hoch, manchmal HTTP, selten FTP).

➡ "Moderate constant SMTP, constant HTTP, minimal FTP" (SMTP konstant moderat, konstant HTTP, selten FTP).

➡ "Very variable SMTP, constant HTTP, minimal FTP" (SMTP stark schwankend, konstant HTTP, selten FTP).

☐ Bei vom Benutzer ausgewählten Werten verwendet das Gerät die entsprechenden Einstellungen in den Konfigurationsseiten des Protokolls (auf der Benutzeroberfläche), so daß Sie die gewünschten Konfigurationseinstellungen angeben können.

☐ **HINWEIS:** In den Verwendungsprofilen wird das Mail-Download-Protokoll (POP3) nicht erwähnt, da es in der Regel seltener verwendet wird als die anderen Protokolle. Wie bei den anderen Proxys sind jedoch die genauen Konfigurationseinstellungen für jedes Protokoll zur Änderung auf den Protokollkonfigurationsseiten verfügbar (auf der Benutzeroberfläche), so daß bei Bedarf weitere Anpassungen vorgenommen werden können.

In den folgenden Abschnitten werden die zusätzlichen Informationen beschrieben, die zum Einrichten der verschiedenen Protokolle erforderlich sind: "E-Mail (SMTP)" auf Seite 27, "Dateiübertragung (FTP)" auf Seite 30 und "Mail-Download (POP3)" auf Seite 30.

E-Mail (SMTP)

Um die erforderlichen Zustellmethoden festzulegen, aktivieren Sie die entsprechenden Kontrollkästchen:

☐ Lokal konfigurierte Domänen (siehe unten).

☐ DNS.

Das Gerät verwendet den DNS-Server, den Sie angeben, wenn Sie die Informationen zu der TCP/IP-Adesse angeben (siehe "Netzwerkadressen" auf Seite 21).

☐ Ersatz-Relays (siehe Seite 29.)

Lokal konfigurierte Domänen

Geben Sie folgende Informationen für die Mail-Relays an: Sie können beliebig viele Relays angeben (unten wurde Raum für 15 Relays gelassen). Identifizieren Sie die gängigsten Relays zuerst, da das Gerät die Relays der Reihe nach ausprobiert:

Relay	E-Mail-Domäne		Vollständig qualifizierte Hosts (Mailserver)
Beispiel 1	*meinefirma.com*	➡	*mail.uk.meinefirma.com*
Beispiel 2	*meinefirma.co.uk*	➡	*mail1.us.meinefirma.com* *mail2.us.meinefirma.com*
Beispiel 3	**.meinefirma2.com*	➡	*mail2.us.meinefirma.com*
1		➡	
2		➡	
3		➡	
4		➡	
5		➡	
6		➡	
7		➡	
8		➡	
9		➡	
10		➡	
11		➡	
12		➡	
13		➡	
14		➡	
15		➡	

Ersatz-Relays

Geben Sie folgende Informationen für die Ersatz-Relays an: Sie können beliebig viele Relays angeben (unten wurde Raum für 15 Relays gelassen). Identifizieren Sie die üblichsten Relays zuerst, da das Gerät die Relays der Reihe nach ausprobiert:

Relay	E-Mail-Domäne		Vollständig qualifizierte Hosts
Beispiel 1	*meinefirma.org*	→	*mail.externefirma1.com mail.externefirma2.com*
Beispiel 2	*	→	*postausgang.meinefirma.com*
1		→	
2		→	
3		→	
4		→	
5		→	
6			
7			
8			
9			
10		→	
11		→	
12		→	
13		→	
14		→	
15		→	

Dateiübertragung (FTP)

Wenn Sie den 8-Bit-ASCII-Mode sperren möchten, aktivieren Sie folgendes Kontrollkästchen:

➡ "Block 8-bit data transfer in ASCII mode" (8-Bit-Datenübertragung im ASCII-Modus sperren).

❑ **HINWEIS:** Manche Dienstprogramme zur Dateiübertragung verwenden standardmäßig den 8-Bit ASCII-Modus. Denken Sie daher daran, diese Dienstprogramme auf den Binärmodus umzuschalten, falls das Gerät den 8-Bit-ASCII-Modus blockiert.

Weitere Informationen zu FTP finden Sie im WebShield e500-Produkthandbuch.

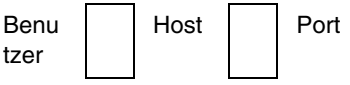
Mail-Download (POP3)

Generischer Proxy

Wenn über das Gerät eine generische Proxy-Verbindung hergestellt wird, trennt das Gerät den Benutzernamen, den Hostnamen und die Port-Nummer mit den Begrenzungszeichen Raute (#) und Doppelpunkt (:) wie im folgenden Beispiel:

```
Benutzer#Host:Port
```

Wenn Sie andere Begrenzungszeichen verwenden möchten, geben Sie diese hier an:



❑ **HINWEIS:** Da Sie Ihr Gerät mit einer Port-Nummer für generische Verbindungen konfigurieren, müssen Ihre POP3-Clients (Software) diese Port-Nummer nicht jedes mal angeben, wenn sie über das Gerät eine generische POP3-Verbindung herstellen.

Dedizierter Proxy

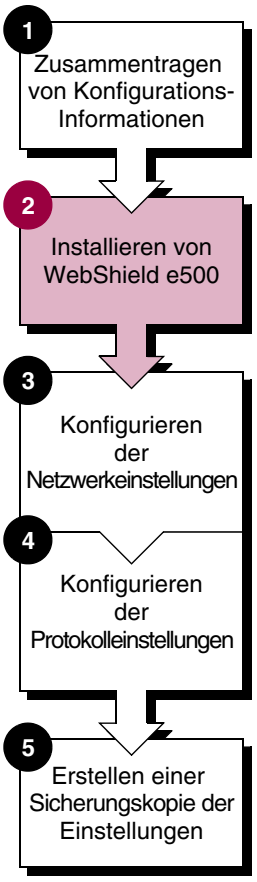
Stellt ein Benutzer über das Gerät eine dedizierte Proxy-Verbindung her, verwendet das Gerät den angegebenen Port, um den POP3-Server zu erreichen.

Sie können Verbindungen zu beliebig vielen Servern ermöglichen (unten wurde Raum für 10 Server gelassen). Geben Sie für jeden Server die Port-Nummer und den Domänennamen an:

Server	Port	Domänenname des POP3-Servers
Beispiel	*1024*	*pop3server.externefirma.com*
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Weitere Informationen zu POP3 finden Sie im WebShield e500-Produkthandbuch.

Installation des McAfee WebShield e500



Wenn alle benötigten Konfigurationsinformationen bereitliegen (siehe Seite 20), können Sie den McAfee WebShield e500 am gewünschten Ort installieren, indem Sie die erforderlichen Verbindungen herstellen (Schritt 2).

In diesem Kapitel werden die Installationsschritte beschrieben. Wir empfehlen Ihnen, diese Anweisungen vor der Installation aufmerksam zu lesen, damit Sie über den Installationsablauf informiert sind.

Eine Liste der zusätzlich erforderlichen Objekte finden Sie auf Seite 12.

Schritt 3 – Konfigurieren der Netzwerkeinstellungen. Eine Beschreibung hierzu finden Sie auf Seite 36.

Weitere Informationen zu den Ports und Steckern des McAfee WebShield e500 finden Sie auf Seite 15.

So installieren Sie den McAfee WebShield e500:

1. Lesen Sie die Warnhinweise in "Informationen zu Stromversorgung und Sicherheit" auf Seite 3, und denken Sie daran, diese Hinweise stets zu befolgen.
2. Nehmen Sie den McAfee WebShield e500 aus der Schutzverpackung und legen Sie ihn auf eine ebene Fläche.
3. Soll der McAfee WebShield e500 an einem bestimmten Ort eingebaut werden (beispielsweise auf ein 19-Zoll-Gestell), führen Sie die folgenden Schritte durch, um sicherzustellen, daß alle Warnhinweise befolgt werden (siehe "Informationen zu Stromversorgung und Sicherheit" auf Seite 3):

   a. Bereiten Sie den vorgesehenen Einbauort vor.

      Sie können den Montagerahmen verwenden, um den McAfee WebShield e500 in einem 19-Zoll-Gestell zu installieren. Befolgen Sie die Anweisungen auf Seite viii (am Anfang dieses Handbuchs).

      Achten Sie bei der Installation des Geräts auf eine ausreichende Belüftung und guten Zugang zu den Ports und Steckern.

   b. Bringen Sie den McAfee WebShield e500 in Einbaulage.

      Achten Sie auf eine sichere Befestigung des Geräts, so daß es nicht herausfallen kann.

4. Stellen Sie mit den mitgelieferten Netzwerkkabeln eine Verbindung zwischen dem Gerät und dem Netzwerk her. Welche Ports und Kabel Sie verwenden, hängt vom Betriebsmodus des Geräts ab:

   - **Proxymodus**

     LAN1-Port: Verwenden Sie das im Lieferumfang enthaltene blaue Netzwerkkabel (oder ein entsprechendes Ethernet-Kabel der Kat 5), um den LAN1-Port (siehe H auf Seite 18) mit dem Netzwerk zu verbinden (Abbildung 2-2). Bei diesem Kabel handelt es sich um ein direkt durchgehendes (ungekreuztes) Kabel. Mit diesem Kabel können Sie den McAfee WebShield e500 mit einem normalen, ungekreuzten (MDI) RJ-45-Port Ihres Netzwerks verbinden.

     Über diese Verbindung können Sie das Gerät über das Netzwerk auch von einem Remote-Computer aus steuern.

     LAN2-Port: Im Proxymodus wird der LAN2-Port zum dedizierten Verwaltungs-Port. Wenn das Gerät für den lokalen Einsatz bestimmt ist, verwenden Sie das orangefarbene Netzwerkkabel (oder ein entsprechendes Ethernet-Crossover-Kabel der Kat 5), um den LAN2-Port (siehe I auf Seite 19) mit der Netzwerkkarte Ihres lokalen Computers zu verbinden (Abbildung 2-2).

     Diese Verbindung muß nur dann hergestellt werden, wenn der McAfee WebShield e500 lokal verwaltet werden soll.

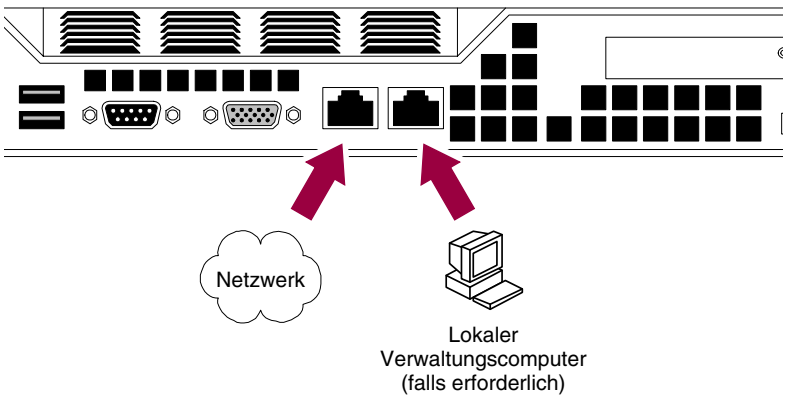


Abbildung 2-2. Verbinden desMcAfee WebShield e500 (Proxymodus)

- **Transparenzmodus**

  Ports LAN1 und LAN2: Verwenden Sie die beiden im Lieferumfang enthaltenen blauen Netzwerkkabel (oder entsprechende Ethernet-Kabel der Kat 5), um den LAN1-Port (siehe H auf Seite 18) und den LAN2-Port (siehe I auf Seite 19) mit Ihrem Netzwerk zu verbinden (Abbildung 2-3) und das Gerät in den Datenstrom einzubinden. Bei diesen Kabeln handelt es sich um direkt durchgehende (ungekreuzte) Kabel. Mit diesen Kabeln können Sie den McAfee WebShield e500 mit den normalen, ungekreuzten (MDI) RJ-45-Ports Ihres Netzwerks verbinden.

  ☐ **HINWEIS:** Im Transparenzmodus muß das Gerät mit zwei getrennten Subnets verbunden sein.

  Das Gerät muß *innerhalb* Ihrer Firewall installiert werden. Wenn Ihr Netzwerk z. B. über einen Hub und eine Firewall mit dem Internet verbunden ist, haben Sie die Möglichkeit, den WebShield e500 zwischen dem Hub und der Firewall zu installieren (wobei Sie den Hub an den LAN1-Port anschließen und die Firewall an den LAN2-Port).

  Im Transparenzmodus können Sie das Gerät über das Netzwerk von einem Remote-Computer aus steuern. Sie können jedoch keine lokale Verwaltungsverbindung über den LAN2-Port herstellen (diese Verbindungsart ist im Proxymodus verfügbar), da der LAN2-Port für den ein- und ausgehenden Datenverkehr benötigt wird.

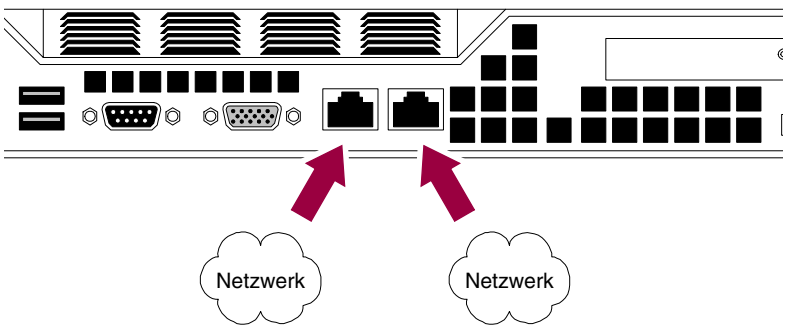


Abbildung 2-3. Verbinden desMcAfee WebShield e500 (Transparenzmodus)

5. Verwenden Sie das im Lieferumfang enthaltene Netzkabel, um den Netzanschluß des McAfee WebShield e500 (siehe D auf Seite 17) mit einer Netzsteckdose zu verbinden.

WICHTIG: Prüfen Sie, ob das im Lieferumfang enthaltene Netzkabel für die Verwendung in Ihrem Land geeignet ist. Anderenfalls wenden Sie sich an Ihren Händler.

Die Gerätesoftware ist bereits vorinstalliert. Legen Sie daher keine CD in das CD-ROM-Laufwerk des Geräts ein, es sei denn, Sie werden ausdrücklich dazu aufgefordert.

---

6. Schalten Sie den McAfee WebShield e500 ein, indem Sie sowohl den Netzschalter als auch den Ein-/Ausschalter auf die Position EIN stellen (Abbildung 2-4).

   Der Netzschalter befindet sich auf der Rückseite des Geräts (siehe E auf Seite 17). Der Ein-/Ausschalter befindet sich im Bedienfeld auf der Vorderseite des Geräts (siehe C auf Seite 16).

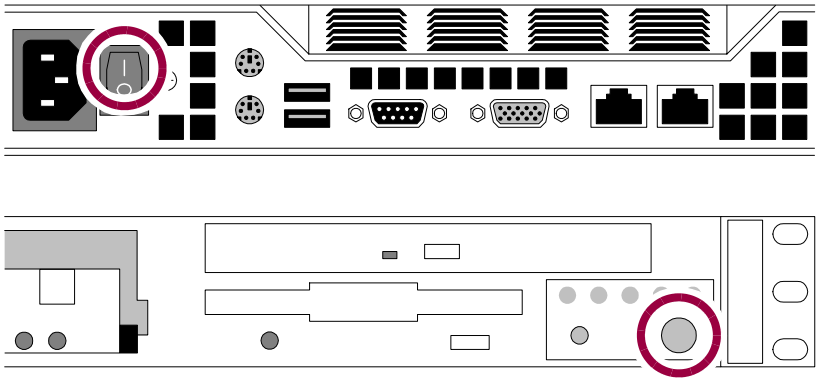
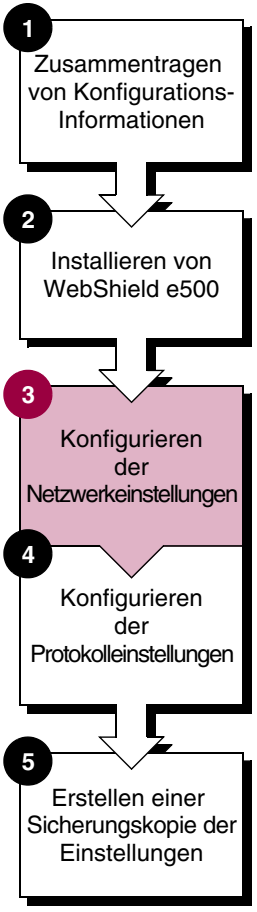


Abbildung 2-4. Einschalten des Geräts

Das Gerät führt die Startsequenz aus und ist nach etwa zwei Minuten einsatzbereit. Sie können jetzt die Netzwerkeinstellungen des WebShield e500 konfigurieren. Anweisungen hierzu finden Sie unter Seite 36.

Konfigurieren der Netzwerkeinstellungen



Nachdem Sie den WebShield e500 installiert und die erforderlichen Verbindungen hergestellt haben (siehe Seite 32), können Sie damit beginnen, die Netzwerkeinstellungen des Geräts zu konfigurieren (Schritt 3).

In diesem Abschnitt werden die Schritte beschrieben, die zur Konfiguration der Netzwerkeinstellungen erforderlich sind. Wir empfehlen Ihnen, diese Anweisungen vor der Konfiguration aufmerksam zu lesen, damit Sie wissen, welche Anforderungen gestellt werden.

Wenn Sie die erforderlichen Konfigurationsinformationen bereits zusammengetragen haben (siehe Seite 20), können Sie den WebShield e500 schneller konfigurieren.

Auf Seite 64 können Sie nachlesen, wie die Software des WebShield e500 wiederhergestellt oder aktualisiert wird.

Wenn Sie bereits Konfigurationsdateien erstellt haben, aus denen die Einstellungen des WebShield e500 wiederhergestellt werden sollen, lesen Sie "Wiederherstellen der Einstellungen" auf Seite 62.

Schritt 4 – Konfigurieren der Protokolleinstellungen. Eine Beschreibung hierzu finden Sie auf Seite 45.

Weitere Informationen zu den Standardeinstellungen finden Sie in Anhang A im Produkthandbuch.

So konfigurieren Sie die Netzwerkeinstellungen des WebShield e500:

1. Öffnen Sie den Web-Browser auf dem Computer, den Sie zur Verwaltung des WebShield e500 verwenden möchten.
2. Geben Sie die folgende Adresse in das Adreßfeld ein (das Feld, in das Sie eine URL (Uniform Resource Locator) zur Anzeige einer Website eingeben):

   `https://<IP-Adresse>`

   HINWEIS: Achten Sie darauf, daß Sie `https` und nicht nur `http` eingeben.

Die einzugebende <IP-Adresse> hängt davon ab, wie die Verbindung zum WebShield e500 hergestellt wird:

- Remote (über das Netzwerk) über den LAN1-Port. Verwenden Sie hierzu die IP-Adresse des LAN1-Port, die Sie für den WebShield e500 konfiguriert haben (die voreingestellte Standard-IP-Adresse ist `10.1.1.108`).
- Remote (über das Netzwerk) über den LAN2-Port (nur im Transparenzmodus verfügbar). Verwenden Sie hierzu die IP-Adresse des LAN2-Port, die Sie für den WebShield e500 konfiguriert haben (die voreingestellte Standard-IP-Adresse ist `10.1.2.108`).
- Lokal, direkt über den LAN2-Port (nur im Proxymodus verfügbar). Verwenden Sie hierzu die IP-Adresse des LAN2-Port, die Sie für den WebShield e500 konfiguriert haben (die voreingestellte Standard-IP-Adresse ist `10.1.2.108`).

☐ **HINWEIS:** Wenn Sie das Gerät im Transparenzmodus verwenden, verwenden Sie die IP-Adresse des Ports und des Subnets, an die der Verwaltungscomputer angeschlossen ist.

Alle Verwaltungsverbindungen verwenden zur Sicherheit die Secure Sockets Layer-Verschlüsselung (SSL). Die SSL-Verbindung wird geschlossen, wenn Sie die Verwaltungssitzung durch Klicken auf **Log off (Abmelden)** beenden. Darüber hinaus wird die SSL-Verbindung nach 15-minütiger Inaktivität geschlossen, um die Sicherheit bei länger andauernden Verwaltungssitzungen zu gewährleisten.

Wenn Sie neue IP-Adressen für den LAN1- oder den LAN2-Port konfigurieren (Schritt 16 auf Seite 40), werden diese vom WebShield e500 zu den vorhandenen IP-Adressen der Ports *hinzugefügt*. Die Standard-IP-Adressen werden nicht ersetzt. Wenn Sie das Gerät im Proxymodus verwenden, hat der LAN2-Port eine eigene IP-Adresse, die ausschließlich für diesen Port verwendet wird (sie wird vom LAN1-Port nicht erkannt). Sie können diese IP-Adresse deaktivieren. Der LAN2-Port wird für einen direkten Verwaltungszugriff verwendet, falls Sie einmal nicht auf den LAN1-Port zugreifen können.

Achten Sie darauf, daß der WebShield e500 im Web-Browser des Verwaltungscomputers (der Computer, den Sie zur Verwaltung des WebShield e500 einsetzen) nicht als dessen Proxy konfiguriert ist. Anderenfalls arbeitet die Verwaltungsverbindung nicht ordnungsgemäß .

Falls Sie zwischen dem Verwaltungscomputer und dem WebShield e500 einen Proxy einsetzen, muß der WebShield e500 als Übergabe-Host des Proxys konfiguriert werden.

---

3. Hat der Web-Browser den WebShield e500 gefunden, wird eventuell eine Sicherheitswarnung angezeigt, in der Sie gefragt werden, ob Sie das Sicherheitszertifikat des Geräts akzeptieren. Klicken Sie auf **Yes (Ja)**, um das Zertifikat zu akzeptieren.

   ➧ **TIP:** Die Sicherheitswarnung kann bei jedem Start einer Browsersitzung angezeigt werden. Sie können das Zertifikat anzeigen und installieren, so daß es automatisch akzeptiert wird. Dann wird die Sicherheitswarnung nicht jedesmal angezeigt. Klicken Sie dazu im Internet Explorer in der Sicherheitswarnung auf **View Certificate (Zertifikat anzeigen)** und im nächsten Dialogfeld auf **Install Certificate (Zertifikat installieren)**.

   Falls Sie den WebShield e500 gerade eingeschaltet haben, müssen Sie etwa zwei Minuten warten, bis die Startsequenz abgeschlossen ist. Anderenfalls kann der Web-Browser das Gerät nicht im ersten Versuch erkennen. In diesem Fall geben Sie die URL noch einmal ein. Falls Sie noch immer nicht auf die Seite „Log on“ (Anmeldung) zugreifen können, lesen Sie bitte Seite 71.

   Die Seite “ Log on“ (Anmeldung) des WebShield e500 wird angezeigt. Der WebShield e500 prüft den Web-Browser, um sicherzustellen, daß er unterstützt wird und den erforderlichen Code enthält, um auf die Benutzeroberfläche zuzugreifen. Aus diesem Grund werden eventuell einige Sicherheitswarnungen und Download-Dialogfelder angezeigt. Füllen Sie die Dialogfelder wie erforderlich aus.

   ❒ **HINWEIS:** Die Benutzeroberfläche des WebShield e500 benötigt die Java 2-Laufzeitumgebung. Falls Ihr Web-Browser die Java 2-Laufzeitumgebung installieren muß, denken Sie daran, daß diese 5-14 MB umfaßt (je nach den für Ihren Browser erforderlichen Komponenten). Die Installation kann länger dauern, wenn Sie eine langsame Datenverbindung zum WebShield e500 haben.

4. Wählen Sie im **Language (Sprache)** die Sprache aus, in der Ihnen die Benutzeroberfläche des WebShield e500 angezeigt werden soll.

   Dies hat keinen Einfluß auf die Systemsprache; siehe Schritt 14 auf Seite 40.

5. Wenn Sie Englisch auswählen, müssen Sie sich für eine regionale Version entscheiden. D. h. Sie müssen keinen englischen Zeichensatz verwenden, wenn Sie die Benutzeroberfläche verwenden.

6. Klicken Sie auf **Log on (Anmeldung)**.

   Das Dialogfeld " Enter Network Password" (Netzwerkkennwort eingeben) wird angezeigt. Sie werden zur Eingabe Ihres Benutzernamens und Kennworts aufgefordert. Der Benutzername lautet `e500`, das Standardkennwort lautet `e500changeme`. Falls Sie die Software des WebShield e500 vor kurzem wiederhergestellt haben, ohne die vorhandenen Einstellungen beizubehalten, wird das Kennwort auf das Standardkennwort zurückgesetzt.

7. Geben Sie Benutzernamen und Kennwort ein, und klicken Sie auf **OK (OK)**.

   Die Benutzeroberfläche des WebShield e500 wird geöffnet und die Seite "System Configuration" (Systemkonfiguration) angezeigt.

   Falls der WebShield e500 bereits konfiguriert wurde, wird die Seite "System Status" (Systemstatus) mit einer Navigationsleiste auf der linken Seite angezeigt. Klicken Sie auf der Navigationsleiste auf **System Configuration (Systemkonfiguration)**. Die Seite „System Configuration" (Systemkonfiguration) wird angezeigt. Weitere Informationen zur Benutzeroberfläche finden Sie unter "Verwenden des WebShield e250" auf Seite 59. Weitere Informationen zur Konfiguration einer bestimmten Seite finden Sie im Hilfethema für diese Seite. Klicken Sie dazu auf die Schaltfläche "Help" (Hilfe).

   ☐ **HINWEIS:** Falls bereits eine Konfigurationsdatei einer früheren WebShield-Version existiert, können Sie diese Einstellungen im Bereich "Konfiguration wiederherstellen" übernehmen. Weitere Informationen hierzu finden Sie unter "Wiederherstellen der Einstellungen" auf Seite 62.

   ---

8. Geben Sie einen eindeutigen Hostnamen für den WebShield e500 in das Textfeld **Appliancename (Anwendungsname)** ein. Der Hostname darf nicht mehr als 15 Zeichen umfassen (siehe "Hostname des Geräts" auf Seite 20).

9. Geben Sie die IP-Adresse des lokalen DNS-Servers in das Textfeld **DNS server (DNS-Server)** ein.

10. Geben Sie die Domäne oder Subdomäne, in der sich der WebShield e500 befindet, in das Textfeld **Domain name (Domänenname)** ein. Ein Beispieleintrag wäre `meinefirma.com` (siehe "Domäne" auf Seite 20).

11. Geben Sie die IP-Adresse des lokalen DNS-Servers in das Textfeld **DNS server (DNS-Server)** ein (siehe "Netzwerkadressen" auf Seite 21).

12. Falls der WebShield e500 über ein Standard-Gateway oder einen Router (Firewall) mit dem Netzwerk kommuniziert, geben Sie die IP-Adresse des Gateways oder des Routers in das Textfeld **Default gateway (Standard-Gateway)** ein (siehe "Netzwerkadressen" auf Seite 21).

    Unter bestimmten Umständen benötigt das Gerät evtl. mehr als ein Gateway oder mehrere Router, um mit dem gesamten Netzwerk kommunizieren zu können. In diesem Fall können Sie die zusätzlichen Gateways und Router als statische Routen angeben (siehe Schritt 22 auf Seite 43).

13. Wenn Sie WebShield e500 im Transparenzmodus betreiben möchten, wählen Sie **Enable Transparency (Transparenz aktivieren)**. Anderenfalls lassen Sie das Kontrollkästchen leer. Das Gerät wird dann im Proxymodus betrieben (siehe "Proxy- oder Transparenzmodus?" auf Seite 24).

14. Wählen Sie unter **System Language (Systemsprache)** die Sprache aus, unter der das Gerät arbeiten soll.

    Diese Einstellung wirkt sich auf die Berichte und Meldungen aus, die vom Gerät ausgegeben werden, aber nicht auf Textzeichenketten, die Sie über die Benutzeroberfläche angeben oder ändern können. Diese Einstellung ist unabhängig von der Sprache, in der die Oberfläche angezeigt wird und die Sie beim Anmelden am Gerät auswählen (siehe Schritt 4 auf Seite 38).

15. Wenn das Feld "LAN-IP-Adressen" nicht sichtbar sind, klicken Sie auf **LAN IP Addresses (LAN-IP-Adressen)**. Die IP-Adressen werden Ihnen dann angezeigt.

    In diesem Feld sind die IP-Adressen aufgeführt, die für die Ports LAN1 und LAN2 konfiguriert wurden.

16. Benützen Sie die Schaltfläche **Add (Hinzufügen)** unterhalb der Listen LAN1 und LAN2, um neue IP-Adressen für diese Ports anzugeben (siehe "Netzwerkadressen" auf Seite 21).

    Sie können für jeden Port mehrere IP-Adressen angeben. Wenn Sie die Änderungen übernehmen, fügt WebShield e500 diese Adressen zu den Ports hinzu (siehe Schritt 27 auf Seite 44). Die bestehenden IP-Adressen werden nicht von den neuen Adressen überschrieben. Wenn Sie eine IP-Adresse nicht länger benutzen möchten, haben Sie folgende Möglichkeiten:

    - IP-Adressen ändern oder deaktivieren – wählen Sie die IP-Adresse aus der Liste aus und klicken Sie anschließend auf **Modify (Ändern)**. Um die IP-Adresse zu deaktivieren, wählen Sie **Disable network address (Netzwerkadresse deaktivieren)**.

- IP-Adresse löschen – wählen Sie die IP-Adresse aus der Liste aus, und klicken Sie anschließend auf **Delete (Löschen)**.

> **HINWEIS:** Wir empfehlen Ihnen, daß Sie mit der neuen IP-Adresse des Daten-Ports (nach der Erstkonfiguration) auf den WebShield e500 zugreifen, *bevor* Sie die Standard-IP-Adresse löschen. So stellen Sie sicher, daß die neue IP-Adresse ordnungsgemäß verwendet werden kann.

Wenn Sie das Gerät im Proxymodus betreiben, wird der LAN2-Port zum dedizierten Verwaltungs-Port. Dadurch können Sie eine direkte Verwaltungsverbindung herstellen.

17. Durch das Deaktivieren des LAN2-Ports können Sie direkte Verwaltungsverbindungen mit dem Gerät verhindern. Wählen Sie hierzu in der LAN2-IP-Adressen-Liste **Disable (Deaktivieren)**.

> **WICHTIG:** Deaktivieren Sie den LAN2-Port **nicht**, wenn Sie den Transparenzmodus eingestellt haben.

Der WebShield e500 verwendet die Listen “Inside Networks“ (Interne Netzwerke) und “Outside Networks“ (Externe Netzwerke), um festzustellen, ob der Datenverkehr über den WebShield e500 von einer internen oder externen Quelle stammt.

> **TIP:** Falls Sie bestimmte interne Subdomänen haben, die als externe Netzwerke behandelt werden sollen (beispielsweise `test.meinefirma.com`), können Sie die Listen “Inside Networks“ (Interne Netzwerke) und “Outside Networks“ (Externe Netzwerke) folgendermaßen verwenden:
>
> Interne Netzwerke:
>
> ```
> *.meinefirma.com
> ```
>
> Externe Netzwerke:
>
> ```
> test.meinefirma.com
>
> *
> ```

18. Klicken Sie auf **Inside Networks (Interne Netzwerke)**. Der Bereich “Inside Networks“ (Interne Netzwerke) wird angezeigt.

19. Geben Sie hier die Domänen oder Subnets der internen Netzwerke Ihrer Firma (innerhalb der Firewall) an, die WebShield e500 schützen soll (siehe “Interne Netzwerke“ auf Seite 21). Sie können beliebig viele Netzwerke angeben.

    HINWEIS: Falls Sie mit dem WebShield e500 die gesamte Domäne schützen möchten, in der sich das Gerät befindet, (angegeben unter Schritt 10 auf Seite 39), muß diese Domäne der Liste “Inside Networks“ (Interne Netzwerke) hinzugefügt werden.

    Klicken Sie zum Hinzufügen eines Netzwerks auf **Add (Hinzufügen)**, und geben Sie dann entweder die Domäne oder deren IP-Adresse und die Subnet-Maske in das Dialogfeld “Add“ (Hinzufügen) ein. Klicken Sie auf **OK** , um die Domäne der Liste “Inside Networks“ (Interne Netzwerke) hinzuzufügen.

20. Klicken Sie auf **Outside Networks (Externe Netzwerke)**. Der Bereich „Outside Networks“ (Externe Netzwerke) wird angezeigt.

    Hier werden die Netzwerke angezeigt, die als Netzwerke außerhalb von WebShield e500 konfiguriert wurden. In der Standardeinstellung des WebShield e500 wird in der Liste der Externen Netzwerke das Platzhaltersymbol * verwendet, um anzuzeigen, daß alle Netzwerke externe Netzwerke sind (mit Ausnahme derjenigen, die in der Liste der Internen Netzwerke aufgeführt sind).

    WICHTIG: Es wird empfohlen, den * -Domäneneintrag in Ihren externen Netzwerken zu behalten, weil dadurch sichergestellt wird, daß das Gerät stellvertretend Datenverkehr für das Internet empfängt.

    Vergessen Sie nicht, auch die IP-Adresse für Ihre Firewall anzugeben.

21. Geben Sie in diesem Bereich die Domänen oder IP-Subnets der externen Netzwerke außerhalb der Firma an (außerhalb der Firewall). Sie können beliebig viele Netzwerke angeben (siehe “Externe Netzwerke“ auf Seite 23).

    Klicken Sie zum Hinzufügen eines Netzwerks auf **Add (Hinzufügen)**, und geben Sie dann entweder die Domäne oder deren IP-Adresse und die Subnet-Maske in das Dialogfeld “Add“ (Hinzufügen) ein. Klicken Sie auf **OK** , um das Netzwerk der Liste “Outside Networks“ (Externe Netzwerke) hinzuzufügen.

22. Um die statischen Routen für verschiedene Teilbereiche des Netzwerks anzugeben, die WebShield e500 für den Zugang benötigt (siehe “Statische Routen und dynamisches Routing“ auf Seite 25), klicken Sie auf **Static Routes (Statische Routen)** und geben die entsprechenden Routen im Bereich “Static Routes„ (Statische Routen) ein.

23. Wenn Sie das Gerät im Transparenzmodus betreiben und dynamisches Routing verwenden möchten, klicken Sie auf **Dynamic Routes (Dynamisches Routing)** und wählen **Enable Dynamic Routing (Dynamisches Routing aktivieren)**.

    Beim dynamischen Routing können die Netzwerkgeräte (einschließlich dieses Geräts) die von den Routern in Ihrem Netzwerk ausgesendeten Routing-Informationen überwachen. Beachten Sie, daß das Gerät nur die Routing-Protokolle RIP (Routing Information Protocol) und OSPF (Open Shortest Path First) unterstützt.

24. Um den Bereich für die Zeit- und Kennworteinstellungen anzuzeigen, klicken Sie auf **Time and Password Settings (Zeit- und Kennworteinstellungen)**.

25. Ändern Sie die Werte für **Time zone (Zeitzone)**, **Date (Datum)** und **Time (Uhrzeit)** so, daß die aktuellen Werte widergespiegelt werden, und klicken Sie dann auf **Set now (Jetzt festlegen)**. Die Uhrzeit wird im 24-Stunden-Format angezeigt.

    Der WebShield e500 ändert Datum und Uhrzeit im eigenen System. Diese Werte werden für Datenverkehr, der das Gerät durchläuft, für Protokolle und Warnungen als Zeitmarke verwendet.

26. Geben Sie zum Ändern des Kennworts das neue Kennwort in das Textfeld **Password (Kennwort)** ein, und bestätigen Sie es im Textfeld **Confirm (Bestätigen)**. Klicken Sie auf **Set now (Jetzt festlegen)**.

WICHTIG: Aus Sicherheitsgründen empfehlen wir Ihnen, das Standardkennwort unverzüglich zu ändern (wenn Sie WebShield e500 zum ersten Mal konfigurieren).

---

27. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

    Der Web-Browser sendet Ihre Änderungen an den WebShield e500. Die Benutzeroberfläche fordert Sie auf, die Software des WebShield e500 neu zu starten, da Änderungen an der IP-Konfiguration vorgenommen wurden.

28. Klicken Sie auf **Restart now (Neustart jetzt ausführen)**.

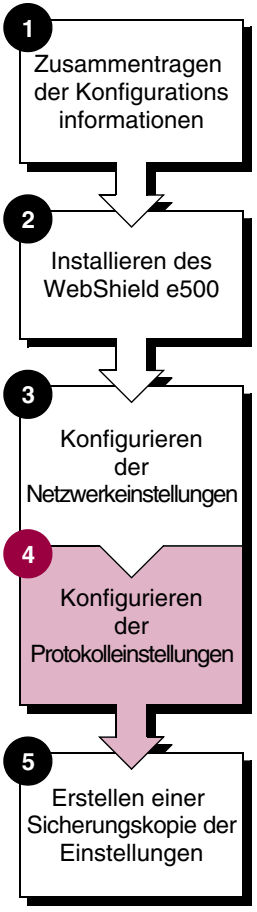
    Der WebShield e500 startet die Software neu und ist nach etwa zwei Minuten einsatzbereit.

    Die Benutzeroberfläche zeigt einen neue URL-Hotlink an, mit dem Sie unter Verwendung der neuen IP-Adresse erneut auf die Benutzeroberfläche zugreifen können.

29. Nach dem Neustart des WebShield e500 klicken Sie auf den URL-Hotlink oder verwenden eine der anderen IP-Adressen, die für den Port konfiguriert wurden, über den das Gerät verwaltet wird. Falls Sie den LAN2-Port verwenden, dessen IP-Adresse jedoch deaktiviert ist (siehe Schritt 17 auf Seite 41), greifen Sie über den LAN1-Port auf das Netzwerk zu.

    Sollten Sie bereits angemeldet sein, wird die Seite “System Status“ (Systemstatus) mit einer Navigationsleiste auf der linken Seite angezeigt. Sie können jetzt die Protokolleinstellungen des WebShield e500 konfigurieren. Anweisungen hierzu finden Sie unter “Konfigurieren der Protokolleinstellungen“ auf Seite 45.

Konfigurieren der Protokolleinstellungen



Nach Abschluß der Konfiguration der Netzwerkeinstellungen des WebShield e500 (siehe Seite 36) können Sie mit der Konfiguration der Protokolleinstellungen beginnen (Schritt 4).

In diesem Abschnitt werden die Schritte beschrieben, die zur Konfiguration der Protokolleinstellungen erforderlich sind. Wir empfehlen Ihnen, diese Anweisungen vor der Konfiguration aufmerksam zu lesen, damit Sie wissen, welche Anforderungen gestellt werden.

Wenn Sie die erforderlichen Konfigurationsinformationen bereits zusammengetragen haben (siehe Seite 20), können Sie den WebShield e500 schneller konfigurieren.

Schritt 5 – Erstellen einer Sicherungskopie der Geräteeinstellungen – ist auf Seite 61beschrieben.

Aufgaben

Dieser Abschnitt ist in die folgenden Aufgaben unterteilt, die Sie in der angegebenen Reihenfolge ausführen müssen:

1. Konfigurieren der Protokolle des WebShield e500 (siehe Seite 46).
2. Konfigurieren der Funktion zum automatischen Aktualisieren, so daß WebShield e500 die Virusdefinitionsdatei (.DAT) und das Scan Modul aktualisieren kann. Nur so bleibt der volle Virenschutz gewährleistet (siehe Seite 52).
3. Gegebenenfalls müssen Sie die Firewall, den Mailserver, den Web-Cache und weitere Geräte so konfigurieren, daß Protokollverkehr durch das Gerät geleitet wird (siehe Seite 53).
4. Testen Ihrer Konfiguration, um sicherzustellen, daß eingehender und ausgehender Datenverkehr ordnungsgemäß auf Virusinfektionen gescannt wird (siehe Seite 55).

Konfigurieren der Protokolle des WebShield e500

Der WebShield e500 stellt Proxy-Dienste für die Protokolle SMTP, FTP, HTTP und POP3 zur Verfügung. In der Standardeinstellung teilt es seine Ressourcen zwischen den Proxies auf und führt eine Virusprüfung des eingehenden und ausgehenden Datenverkehrs durch (die Richtungen des Datenverkehrs werden bei POP3 nicht unterschieden). Weitere Informationen zu Proxies und Protokollen finden Sie unter "Ports und Stecker" auf Seite 15.

So konfigurieren Sie, welche Protokolle aktiviert und auf Viren geprüft werden, und wählen das geeignete Verwendungsprofil:

1. Deaktivieren Sie auf der Seite "System Configuration" (Systemkonfiguration) die entsprechenden Kontrollkästchen im Bereich **Protocols enabled (Aktivierte Protokolle)**, um die Proxy-Dienste für diese Protokolle auszuschließen (). So verhindern Sie, daß der Protokollverkehr über den WebShield e500 geleitet wird.

   HINWEIS: Im Transparenzmodus wird dadurch nicht verhindert, daß Datenverkehr durch das Gerät geleitet wird.

2. Zur Deaktivierung der Virenprüfung von ein- oder ausgehendem Datenverkehr für eines der aktivierten Protokolle wählen Sie auf der Navigationsleiste die entsprechende **Configuration page (Konfigurationsseite)** aus ("E-mail Configuration" [E-Mail-Konfiguration], "File Transfer Configuration" [Konfiguration der Dateiübertragung], "Web Browsing Configuration" [Konfiguration für das Surfen im Internet] oder "Mail Download Configuration" [Konfiguration der Mail-Downloads]), dann deaktivieren Sie entweder **Scan inbound traffic (Eingehende Nachrichten scannen)** oder **Scan outbound traffic (Ausgehende Nachrichten scannen)** (**Scan POP3 traffic [POP3-Mail scannen]** wird auf der Seite "Mail Download Configuration" [Konfiguration der Mail-Downloads] verwendet).

   WARNUNG: Deaktivieren Sie die Virenprüfung nicht für aktivierte Protokolle, *es sei denn*, deren Datenverkehr wird an einem anderen Punkt im Netzwerk gescannt. Wenn Sie zulassen, daß nicht überprüfter Datenverkehr in Ihr Unternehmen gelangt und es verläßt, öffnen Sie eine Sicherheitslücke für Viren.

   Achten Sie darauf, alle Netzwerkgeräte so zu konfigurieren, daß sie die Protokolle über den WebShield e500 routen (falls erforderlich). Das Gerät sollte von Datenverkehr nicht umgangen werden können (siehe Seite 53).

3. Klicken Sie auf der Navigationsleiste auf **System Profiles (Systemprofile)**.

4. Wählen Sie das am besten geeignete Verwendungsprofil aus (siehe “Scanning profile (Scan-Profil)“ auf Seite 27).

   Die Verwendungsprofile erwähnen das Mail-Download-Protokoll (POP3) nicht, da es eine weitaus geringere Bandbreite als die anderen Protokolle verwendet. Falls Sie eine Überprüfung des POP3-Protokolls aktiviert haben, wird es ungeachtet des ausgewählten Profils gescannt.

   Sie können einen beliebigen Verwendungswert (einschließlich der POP3-Ebenen) auf den Konfigurationsseiten der Protokolle anpassen. In diesem Fall wählt der WebShield e500 auf der Seite “System Profiles“ (Systemprofile) automatisch die Einstellung **Vom Benutzer ausgewählte Werte der Konfigurationsseiten für die verschiedenen Protokolle**.

5. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

Konfigurieren der für die Protokolle verwendeten Ports

Der WebShield e500 verwendet die folgenden Standard-Ports für die Protokolle:

- E-Mail (SMTP): 25
- Dateiübertragung (FTP): 21
- Web-Browsing (HTTP): 80
- Mail-Download (POP3): 110

Falls das Netzwerk in Ihrem Unternehmen andere Ports für die Protokolle verwendet, müssen Sie die Port-Nummern am WebShield e500 entsprechend ändern.

So ändern Sie den für ein Protokoll verwendeten Port:

1. Klicken Sie auf der Navigationsleiste auf die **Configuration page (Konfigurationsseite)** des gewünschten Protokolls.

2. Geben Sie die erforderliche Port-Nummer in das Textfeld **Port on which to listen... (Port, an dem ... empfangen werden)** ein (siehe “Protokolle“ auf Seite 26).

3. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

Konfigurieren der Zustellmethoden für E-Mail (SMTP)

Bei aktiviertem E-Mail-Protokoll (die Standardeinstellung) müssen Sie die verwendeten Zustellmethoden konfigurieren.

In diesem Abschnitt finden Sie nur die zum Einrichten der E-Mail-Zustellmethoden erforderlichen Informationen, damit der WebShield e500 mit der Überprüfung und Zustellung der Daten beginnen kann. Für dieses Protokoll gibt es mehrere Seiten mit Funktionen. Einzelheiten zur Konfiguration dieser Seiten finden Sie in den entsprechenden Hilfethemen, die Sie durch Klicken auf die Schaltflächen "Help" (Hilfe) aufrufen können (siehe Seite 59).

So konfigurieren Sie die E-Mail-Zustellmethoden:

1. Klicken Sie auf der Navigationsleiste auf **E-mail Delivery (Zustellung von E-Mail-Nachrichten)**.
2. Wählen Sie die erforderlichen Zustellmethoden im Dialogfeld "Methods Used" (Verwendete Methoden) aus (siehe "E-Mail (SMTP)" auf Seite 27).
3. Falls Sie die Zustellmethode **Local domains (Lokale Domänen)** gewählt haben, klicken Sie auf **Local domains (Lokale Domänen)** und geben dann die Mail-Relays in das Dialogfeld ein. Sie können beliebig viele Mail-Relays angeben (siehe "Lokal konfigurierte Domänen" auf Seite 28).

   Die Mail-Relays routen E-Mail-Nachrichten für bestimmte Domänen (beispielsweise myorg.com) an die entsprechenden Mail-Server (beispielsweise mail1.meinefirma.com). Klicken Sie zum Hinzufügen eines Mail-Relays auf **Add (Hinzufügen)**, und geben Sie die E-Mail-Domäne und den Host (Mail-Server) in das Dialogfeld "Add" (Hinzufügen) ein. Klicken Sie auf **OK (OK)**, um die E-Mail-Domäne und den Host der Liste "Local Domains" (Lokale Domänen) hinzuzufügen.

➧ **TIP:** Der WebShield e500 versucht, die Mail-Relays in der angegebenen Reihenfolge anzusprechen. Falls eines der Relays für eine Nachricht erfolgreich angesprochen wurde, werden die übrigen Relays für diese Nachricht nicht mehr versucht. Verwenden Sie daher die Schaltflächen **Move up (Nach oben)** und **Move down (Nach unten)**, um die Relays in der gewünschten Reihenfolge anzuordnen. Setzen Sie die am häufigsten verwendeten Relays an den Anfang der Liste.

---

4. Falls Sie die Zustellmethode **Fallback relays (Ersatz-Relays)** gewählt haben, klicken Sie auf **Fallback relays (Ersatz-Relays)** und geben dann die Ersatz-Relays in das Dialogfeld ein. Sie können beliebig viele Mail-Relays angeben (siehe “Ersatz-Relays“ auf Seite 29).

   Die Ersatz-Relays routen E-Mail-Nachrichten, die mit Hilfe anderer Zustellmethoden nicht zugestellt werden konnten. Klicken Sie zum Hinzufügen eines Ersatz-Relays auf **Add (Hinzufügen)**, geben Sie dann die E-Mail-Domäne und den Host (Mail-Server) in das Dialogfeld „Add“ (Hinzufügen) ein. Klicken Sie auf **OK** , um die E-Mail-Domäne und den Host der Liste “Fallback Relays“ (Ersatz-Relays) hinzuzufügen.

   ➧ **TIP:** Sie können ein Mail-Relay erstellen, um alle Nachrichten aus allen Domänen zu routen. Dazu verwenden Sie für die Domäne den Platzhalter *. Wenn dieser Platzhalter unter den anderen Einträgen in der Liste “Fallback Relays“ (Ersatz-Relays) positioniert wird, versucht der WebShield e500 zunächst die anderen Einträge, bevor er den Platzhaltereintrag versucht.

   Die Liste “Fallback Relays“ (Ersatz-Relays) kann Relays für lokale Hosts (Mail-Server) enthalten. So können Sie *nach* einer DNS-Server-Suche versuchen, mit Hilfe lokaler Domänen nicht zustellbare Nachrichten in das Unternehmen zu routen.

   Der WebShield e500 versucht, die Mail-Relays in der angegebenen Reihenfolge anzusprechen. Falls eines der Relays für eine Nachricht erfolgreich angesprochen wurde, werden die übrigen Relays für diese Nachricht nicht mehr versucht. Verwenden Sie daher die Schaltflächen **Move up (Nach oben)** und **Move down (Nach unten)**, um die Relays in der gewünschten Reihenfolge anzuordnen. Setzen Sie die am häufigsten verwendeten Relays an den Anfang der Liste.

   ---

5. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

Konfigurieren der Zulässigkeit von 8-Bit-Datenübertragungen

Das File Transfer Protocol (FTP) ermöglicht die Übergabe von Daten zwischen Computern in zwei Modi: Binär und 8-Bit-ASCII (American Standard Code for Information Interchange). Eine binäre Übertragung ist auch zwischen Computerplattformen konsistent. Daher können die Daten effizient gescannt werden.

❑ **HINWEIS:** Der WebShield e500 sperrt standardmäßig den 8-Bit ASCII-Übertragungsmodus, da diese Daten unterschiedliche Zeichencodes und Formatierungen enthalten (abhängig von den verwendeten Computersystemen). Darin können sich Viren leicht verbergen.

Wenn das File Transfer Protocol aktiviert ist (die Standardeinstellung), können Sie 8-Bit-Datenübertragungen aktivieren.

So aktivieren Sie 8-Bit-Datenübertragungen:

1. Klicken Sie auf der Navigationsleiste auf **File Transfer Configuration (Konfiguration der Dateiübertragung)**.
2. Deaktivieren Sie das Kontrollkästchen **Block 8-bit data transfer in ASCII mode (8-Bit-Datenübertragung im ASCII-Modus sperren)** (siehe “Dateiübertragung (FTP)“ auf Seite 30).
3. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

   ❑ **HINWEIS:** Manche Dienstprogramme zur Dateiübertragung verwenden standardmäßig den 8-Bit ASCII-Modus. Denken Sie daher daran, diese Dienstprogramme auf den Binärmodus umzuschalten.

Konfigurieren der Mail-Download-Proxys (POP3)

Wenn das Mail Download Protocol aktiviert ist (die Standardeinstellung), können Sie das Begrenzungszeichen (für generische Proxy-Verbindungen) und die Port-Nummern (für dedizierte Proxy-Verbindungen) konfigurieren.

Stellt ein Benutzer dann eine generische Proxy-Verbindung über den WebShield e500 her, trennt das Gerät den Benutzernamen, Hostnamen und die Port-Nummer standardmäßig mit den Begrenzungszeichen Raute (#) und Doppelpunkt (:), wie im folgenden Beispiel dargestellt:

```
Benutzer#Host:Port
```

So ändern Sie die Begrenzungszeichen für generische POP3-Proxy-Verbindungen:

1. Klicken Sie auf der Navigationsleiste auf **Mail Download Configuration (Konfiguration der Mail-Downloads)**.
2. Geben Sie das gewünschte neue Begrenzungszeichen ein (siehe “Generischer Proxy“ auf Seite 30).
3. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

So geben Sie die für dedizierte POP3-Proxy-Verbindungen verwendeten Ports an:

1. Geben Sie auf der Seite „Mail Download Configuration“ (Konfiguration der Mail-Downloads) die Port-Nummern und POP3-Server in die Liste “Dedicated Proxy Connections“ (Dedizierte Proxy-Verbindungen) ein. Sie können beliebig viele Server angeben, die zugeordneten Port-Nummern müssen jedoch eindeutig sein (siehe “Dedizierter Proxy“ auf Seite 31).

   Klicken Sie zum Hinzufügen eines POP3-Servers auf **Add (Hinzufügen)**, und geben Sie dann die eindeutige Port-Nummer (in der Regel zwischen 1024 und 32 767) und den Serverdomänennamen (beispielsweise pop3server.externefirma.com) in das Dialogfeld “Add“ (Hinzufügen) ein. Klicken Sie auf **OK** , um die Port-Nummer und den Serverdomänennamen der Liste “Dedicated Proxy Connections“ (Dedizierte Proxy-Verbindungen) hinzuzufügen.
2. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

Konfigurieren der Funktion zum automatischen Aktualisieren

Die Funktion zum automatischen Aktualisieren hält die Virusdefinitionsdatei (.DAT) und das Scan-Modul stets aktuell. Nur so bleibt der volle Virenschutz gewährleistet.

WICHTIG: Wenn der WebShield e500 (gemäß Ihren Einstellungen) nach Viren sucht, verwendet er das Virensuchmodul und die aktuelle .DAT-Datei zum Suchen und Entfernen von Viren. Täglich werden neue Viren entdeckt. Daher erstellt McAfee neue Definitionsdateien, um einen Schutz vor diesen Viren zu gewährleisten. Darüber hinaus wird von Zeit zu Zeit auch eine neue Version des Scan-Moduls erstellt.

So konfigurieren Sie die Funktion zum automatischen Aktualisieren:

1. Klicken Sie auf der Navigationsleiste auf **Anti-Virus Automatic Updating (Automatisches Aktualisieren der Antiviren-Software)**.
2. Geben Sie im Dialogfeld "FTP Download Site" (FTP-Download-Site) den Speicherort an, von dem die .DAT-Datei und das Scan-Modul kopiert werden sollen. In der Standardeinstellung ruft der WebShield e500 die .DAT-Datei und das Scan-Modul vom FTP-Server von Network Associates (ftp.nai.com) ab.

   Wenn ein anderer FTP-Server verwendet wird, ändern Sie die folgenden Textfelder:

   - **Server name (Servername)**
   - **Path to .DAT/engine files (Pfad zu DAT-/Moduldateien)**
   - **Server user name (Server-Benutzername)** (falls erforderlich)
   - **Password (Kennwort)** (falls erforderlich)

   Falls Ihre Verbindung über einen Proxy-Server erfolgt, müssen Sie Informationen zu diesem Server in die folgenden Textfelder eingeben:

   - **Proxy server (Proxy-Server)**
   - **Proxy port number (Port-Nummer des Proxys)**
   - **Proxy user name (Proxy-Benutzername)** (falls erforderlich)
   - **Proxy password (Proxy-Kennwort)** (falls erforderlich)

   Weitere Informationen zur Konfiguration dieser Seite finden Sie in den Hilfethemen. Klicken Sie dazu auf die Schaltfläche "Help" (Hilfe) .

3. Klicken Sie auf **FTP Update Schedule (FTP-Aktualisierungsplan)**, und stellen Sie die Tage und Uhrzeiten ein (im 24-Stunden-Format), an denen der WebShield e500 die .DAT-Datei und das Scan-Modul aktualisieren soll.

4. Klicken Sie auf **Apply all changes (Alle Änderungen anwenden)**.

   Der Web-Browser sendet Ihre Änderungen an den WebShield e500.

Konfigurieren weiterer Geräte

In diesem Abschnitt finden Sie eine Übersicht der Änderungen, die Sie an Ihren weiteren Geräten vornehmen müssen, damit der WebShield e500 vollständig in das Netzwerk integriert wird. Die Änderungen hängen davon ab, ob Sie WebShield e500 im Proxymodus oder im Transparenzmodus betreiben.

- **Proxymodus** (expliziter Proxy) – Sie müssen alle Netzwerkgeräte so konfigurieren, daß sie die Protokolle über den WebShield e500 routen. Kein Datenverkehr sollte das Gerät umgehen. Hierzu gehört das Konfigurieren aller internen Clients (beispielsweise HTTP-, FTP- und POP3-Software) zum Verwenden des WebShield e500 als Proxy-Server. Insbesondere sollten Sie darauf achten, daß die HTTP-, FTP- und Gopher-Einstellungen Ihrer Web-Clients die HTTP-Port-Nummer verwenden. (siehe unten: “Routen von Protokollen über den WebShield e500,”).

- **Transparenzmodus** (transparenter Proxy) – Im Transparenzmodus kann WebShield e500 physisch in Ihr Netzwerk eingebunden werden, ohne daß alle anderen Netzwerkkomponenten umkonfiguriert werden müssen. Das SMTP-E-Mail-System muß jedoch so konfiguriert werden, daß der E-Mail-Verkehr durch das Gerät geleitet wird (siehe “Modifizieren der DNS-Server-Datensätze“ auf Seite 54).

WICHTIG: Im täglichen Betrieb Ihres E-Mail-Systems müssen Sie den Mail-Server gelegentlich offline schalten, um Änderungen an der Konfiguration oder andere Wartungsaufgaben durchzuführen. Wenn Sie den WebShield e500 aktiviert lassen, wird er weiterhin eingehende E-Mails akzeptieren und auf Viren scannen, aber er kann diese E-Mails nicht weiterleiten (es sei denn, Sie haben einen Backup-Mail-Server in Ihrem E-Mail-Setup angegeben). Sollte der WebShield e500 zuviele Nachrichten erhalten, reicht der Speicherplatz nicht aus. Um dieses Problem zu vermeiden, deaktivieren Sie den SMTP-Proxy am Gerät, wenn der Mail-Server offline geschaltet ist. Ihre Firewall sollte in diesem Fall eingehende Nachrichten als unzustellbar zurücksenden.

Routen von Protokollen über den WebShield e500

Ausführliche Informationen zur Konfiguration der erforderlichen Optionen finden Sie in der mit Ihrem Gerät gelieferten Dokumentation. Nach Abschluß der Konfiguration Ihrer Geräte können Sie die Tests auf Seite 55 durchführen, um sicherzustellen, daß Ihr Mail-Setup ordnungsgemäß arbeitet. Der WebShield e500 verwendet die folgenden Standard-Ports für die Protokolle:

- E-Mail (SMTP): 25
- Dateiübertragung (FTP): 21
- Web-Browsing (HTTP): 80
- Mail-Download (POP3): 110

Falls Sie den WebShield e500 zur Verwendung anderer Ports für die Protokolle konfiguriert haben, müssen Sie Ihre Geräte entsprechend auf diese Ports einstellen.

Darüber hinaus empfehlen wir Ihnen, Ihre Firewall so zu konfigurieren, daß ausschließlich interner Datenverkehr vom WebShield e500 gesendet und empfangen wird (für die Protokolle, für die der WebShield e500 Proxy-Dienste ausführt).

Modifizieren der DNS-Server-Datensätze

Abhängig von der Netzwerktopologie in Ihrem Unternehmen und den Protokollen, für die der WebShield e500 Proxy-Dienste ausführt, müssen Sie eventuell Datensätze für die internen und externen DNS-Server modifizieren (siehe die Szenarios in Kapitel 1 des Produkthandbuchs).

Dies gilt insbesondere dann, wenn Sie interne FTP-, Web- oder POP3-Server haben. Sie müssen eventuell Datensätze für *externe* DNS-Server erstellen, die die internen FTP-, Web- und POP3-Server Ihrer Firewall zuordnen. Bei einem internen Webserver müssen Sie darüber hinaus Datensätze für den *internen* DNS-Server erstellen, die den Domänennamen des Webservers seiner IP-Adresse zuordnen.

Die Datensätze, die Sie auf dem DNS-Server aufnehmen und deren Reihenfolge bestimmen darüber hinaus, ob Sie eine Fail-Over, Fail-Closed oder Fail-Safe-Konfiguration vornehmen müssen (siehe Kapitel 1 des Produkthandbuchs). Aus diesem Grund müssen Sie sicherstellen, daß die Datensätze in der richtigen Reihenfolge aufgeführt werden.

Weitere Informationen zur Modifikation der DNS-Server-Software entnehmen Sie der Dokumentation des DNS-Servers.

Testen Ihrer Konfiguration

Wir empfehlen Ihnen, die folgenden Tests durchzuführen (abhängig von den aktivierten Proxies), um sicherzustellen, daß der WebShield e500 ordnungsgemäß in Ihr Netzwerk integriert ist:

- "Test 1: Überprüfen, ob E-Mail-Nachrichten (SMTP) gescannt und ordnungsgemäß zugestellt werden" auf Seite 56.
- "Test 2: Überprüfen, ob Dateiübertragungen (FTP) ordnungsgemäß gescannt werden" auf Seite 57.
- "Test 3: Überprüfen, ob beim Surfen im Internet (HTTP) ordnungsgemäß gescannt wird" auf Seite 57.
- "Test 4: Überprüfen, ob die Mail-Downloads (POP3) ordnungsgemäß gescannt werden" auf Seite 58.

Diese Tests verwenden eine spezielle Testdatei, die vom European Institute of Computer Anti-virus Research (EICAR), einem Zusammenschluß der Antiviren-Softwarehersteller mit Hauptsitz in Europa, entwickelt wurde.

WICHTIG: Die EICAR-Testdatei *enthält keinen Virus*. Sie kann sich nicht ausbreiten, andere Dateien infizieren oder das System in anderer Weise schädigen. Löschen Sie die Datei nach dem Testen der Installation, damit andere Benutzer nicht verunsichert werden.

Deaktivieren Sie die Antiviren-Software auf dem Computer, auf dem Sie die EICAR-Testdatei erstellen, damit diese nicht von der Antiviren-Software entfernt wird.

So erstellen Sie die EICAR-Testdatei:

1. Öffnen Sie einen Standard-Texteditor, beispielsweise Microsoft Notepad.
2. Erstellen Sie ggf. eine neue Textdatei und geben Sie dann die folgende Textzeile ein:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
   ANTIVIRUS-TEST-FILE!$H+H*
   ```

   HINWEIS: Die obenstehende Zeile muß als eine einzelne Zeile in Ihrem Texteditor erscheinen.

3. Speichern Sie diese Textdatei unter dem Namen EICAR.COM. Die Größe der Datei beträgt ca. 70 Bytes.

Test 1: Überprüfen, ob E-Mail-Nachrichten (SMTP) gescannt und ordnungsgemäß zugestellt werden

Sie können das Scannen auf Viren und die Zustellung von SMTP-Mails durch den WebShield e500 prüfen, indem Sie die EICAR-Testdatei zwischen internen und externen (Internet) E-Mail-Konten versenden.

So prüfen Sie, ob das SMTP-Virenscannen und die Zustellung ordnungsgemäß arbeiten:

1. Melden Sie sich bei einem Computer in Ihrem Netzwerk an, der über ein E-Mail-Konto verfügt.
2. Erstellen Sie die EICAR-Testdatei.
3. Öffnen Sie die E-Mail-Anwendung auf Ihrem Computer und erstellen Sie eine neue Nachricht mit den folgenden Attributen: Geben Sie den beabsichtigten Empfänger als eine externe E-Mail-Adresse im Internet an, auf die Sie Zugriff haben, und hängen Sie die EICAR-Datei an die Nachricht an.
4. Senden Sie die Nachricht.

   Wenn Ihr E-Mail-System ordnungsgemäß konfiguriert ist und der WebShield e500 die Standardeinstellungen aufweist:

   - Der Mail-Server empfängt die ausgehende Nachricht vom internen Computer und stellt sie dem WebShield e500 zu.
   - Der WebShield e500 scannt die Nachricht auf Viren und erkennt und entfernt die angehängte EICAR-Testdatei. Dann gibt er die bereinigte Nachricht an das interne E-Mail-Konto zurück.
5. Prüfen Sie, ob die Nachricht zurückgegeben und die EICAR-Testdatei entfernt wurde.
6. Greifen Sie auf das externe E-Mail-Konto im Internet zu, das Sie für die erste Nachricht angegeben haben, und senden Sie eine ähnliche Nachricht an das interne E-Mail-Konto. Hängen Sie dabei eine neue EICAR-Testdatei an.

   Wenn Ihr E-Mail-System ordnungsgemäß konfiguriert ist und der WebShield e500 die Standardeinstellungen aufweist, empfängt der WebShield e500 die Antwortnachricht. Er scannt die Nachricht auf Viren und erkennt und entfernt die angehängte EICAR-Testdatei. Dann gibt er die bereinigte Nachricht an das externe E-Mail-Konto zurück.
7. Prüfen Sie, ob die Nachricht zurückgegeben und die EICAR-Testdatei entfernt wurde.
8. Löschen Sie die von Ihnen erstellten EICAR-Testdateien.

Test 2: Überprüfen, ob Dateiübertragungen (FTP) ordnungsgemäß gescannt werden

Sie können das FTP-Virenscannen des WebShield e500 überprüfen, indem Sie die EICAR-Testdatei auf einem FTP-Server ablegen und dann versuchen, diese Datei herunterzuladen.

So prüfen Sie, ob das FTP-Virenscannen ordnungsgemäß arbeitet:

1. Melden Sie sich beim FTP-Server an.
2. Erstellen Sie die EICAR-Testdatei.
3. Melden Sie sich bei einem Computer in Ihrem Netzwerk an, der über einen FTP-Client (eine FTP-Software) verfügt.
4. Öffnen Sie den FTP-Client auf dem Computer und stellen Sie eine Verbindung mit dem FTP-Server her.
5. Suchen Sie die EICAR-Testdatei und versuchen Sie, die Datei herunterzuladen.

   Wenn Ihr FTP-System ordnungsgemäß konfiguriert ist, erkennt der WebShield e500 die EICAR-Testdatei und verhindert den Download.
6. Löschen Sie die von Ihnen erstellte EICAR-Testdatei.

Test 3: Überprüfen, ob beim Surfen im Internet (HTTP) ordnungsgemäß gescannt wird

Sie können das HTTP-Virenscannen des WebShield e500 überprüfen, indem Sie von einer Webseite auf einem Webserver auf die EICAR-Testdatei verweisen und dann versuchen, diese Datei herunterzuladen.

So prüfen Sie, ob das HTTP-Virenscannen ordnungsgemäß arbeitet:

1. Melden Sie sich beim Webserver an.
2. Erstellen Sie die EICAR-Testdatei, und erstellen Sie auf einer Webseite eine Verknüpfung zur Testdatei.
3. Melden Sie sich bei einem Computer in Ihrem Netzwerk an, der über einen HTTP-Client (eine Web-Browser-Software) verfügt.
4. Öffnen Sie den HTTP-Client auf dem Computer, und greifen Sie auf die Webseite mit der EICAR-Testdatei zu.
5. Versuchen Sie, die EICAR-Testdatei herunterzuladen.

   Wenn Ihr HTTP-System ordnungsgemäß konfiguriert ist, erkennt der WebShield e500 die EICAR-Testdatei und verhindert den Download.
6. Löschen Sie die von Ihnen erstellte EICAR-Testdatei.

Test 4: Überprüfen, ob die Mail-Downloads (POP3) ordnungsgemäß gescannt werden

Sie können das POP3-Virenscannen des WebShield e500 überprüfen, indem Sie die EICAR-Testdatei in einer Nachricht an ein POP3-E-Mail-Konto senden und dann versuchen, diese Nachricht herunterzuladen.

So prüfen Sie, ob das POP3-Virenscannen ordnungsgemäß arbeitet:

1. Melden Sie sich bei einem Computer in Ihrem Netzwerk an, der über einen nicht gescannten Zugriff auf den POP3-Server verfügt.
2. Erstellen Sie die EICAR-Testdatei, und senden Sie die Datei an ein E-Mail-Konto auf dem POP3-Server.
3. Melden Sie sich bei einem Computer in Ihrem Netzwerk an, der über einen POP3-Client (eine POP3 Mail-Download-Software) verfügt.
4. Laden Sie die Nachrichten für das POP3 E-Mail-Konto herunter, das die Nachricht mit der EICAR-Testdatei enthält.

   Wenn Ihr POP3-System ordnungsgemäß konfiguriert ist, erkennt der WebShield e500 die EICAR-Testdatei und löscht sie aus der Nachricht.
5. Prüfen Sie, ob die EICAR-Testdatei aus der Nachricht entfernt wurde.
6. Löschen Sie die von Ihnen erstellte EICAR-Testdatei.

Verwenden des WebShield e250

Die Benutzeroberfläche des WebShield e500 (siehe Seite x am Anfang dieses Handbuchs) wurde speziell konzipiert, um Ihnen das schnelle und einfache Konfigurieren der Einstellungen zu ermöglichen.

A Navigationsleiste

Auf der Navigationsleiste finden Sie die Funktionen, bei denen eine Konfiguration möglich ist (diese Funktionen sind durch einen Pfeil ▸ gekennzeichnet). Klicken Sie auf eine Funktion, um die zugehörige Seite mit den Einstellungen anzuzeigen.

B Seite

Die Seite zeigt die Einstellungen der auf der Navigationsleiste ausgewählten Funktion. Diese Einstellungen können sowohl angezeigt als auch geändert werden.

HINWEIS: Die von Ihnen vorgenommenen Änderungen werden erst dann für den WebShield e500 übernommen, wenn Sie auf **Apply all changes (Alle Änderungen anwenden)** klicken.

Jede Seite enthält die folgenden Schaltflächen:

Product guide (Produkthandbuch) – Nach dem Klicken auf diese Schaltfläche wird eine PDF-Version (Portable Document Format) des WebShield e500-Produkthandbuchs angezeigt.

Help (Hilfe) – Nach dem Klicken auf diese Schaltfläche wird das Hilfethema zur aktuellen Seite in einem neuen Browserfenster angezeigt. Das Hilfethema enthält ausführliche Informationen sowie einige Tips zur Optimierung der Funktionen des WebShield e500.

Cancel (Abbrechen) – Nach dem Klicken auf diese Schaltfläche werden alle Änderungen widerrufen, die Sie nach der letzten Übernahme von Änderungen auf der *aktuellen* Seite vorgenommen haben. Wenn Sie zu einer anderen Seite wechseln, speichert der Web-Browser die auf der Seite vorgenommenen Änderungen. Zum Widerrufen der Änderungen müssen Sie auf die Schaltfläche **Cancel all changes (Alle Änderungen verwerfen)** klicken.

C Dialogfeld

Einige Seiten haben Dialogfelder, in denen weitere Felder enthalten sind. Wählen Sie die Optionen auf der Seite, um die Dialogfelder anzuzeigen.

D Steuerungsschaltflächen

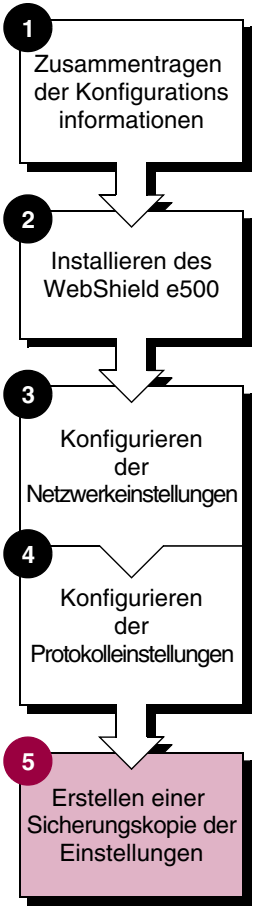
Die Benutzeroberfläche enthält die folgenden Steuerungsschaltflächen:

- **Log off (Abmelden)** – Beendet die Verwaltungssitzung. Sie kehren zur Seite "Log on" (Anmeldung) zurück und müssen sich erneut mit Ihrem Kennwort anmelden, um weitere Konfigurationen am WebShield e500 vorzunehmen.
- **Apply all changes (Alle Änderungen anwenden)** – Mit dieser Schaltfläche übernehmen Sie alle Änderungen, die Sie an der Konfiguration des WebShield e500 vorgenommen haben.
- **Cancel all changes (Alle Änderungen verwerfen)** – Mit dieser Schaltfläche verwerfen Sie die Änderungen auf *allen* Seiten, die Sie nach der letzten Übernahme von Änderungen für den WebShield e500 vorgenommen haben. Falls Sie auf mehreren Seiten Änderungen vorgenommen haben, werden alle Änderungen verworfen.

In diesem Handbuch werden nicht alle Seiten der Benutzeroberfläche ausführlich beschrieben. Diese Informationen finden Sie jedoch in den entsprechenden Hilfethemen.

Sichern und Wiederherstellen der Einstellungen

Nach Abschluß der Konfiguration des WebShield e500 sollten Sie eine Sicherungskopie der Einstellungen anlegen. So können Sie die Einstellungen im unwahrscheinlichen Fall eines Problems schnell wiederherstellen, falls die Software des WebShield e500 neu installiert werden muß. Einzelheiten zum Wiederherstellen der Gerätesoftware finden Sie unter “Wiederherstellen und Aktualisieren der Gerätesoftware“ auf Seite 64.



Sichern Ihrer Einstellungen

So speichern Sie die Geräteeinstellungen in einem Satz von Konfigurationsdateien:

1. Öffnen Sie den Web-Browser auf dem Computer, auf dem Sie die Sicherungskopie der Konfigurationsdateien erstellen möchten.
2. Greifen Sie mit der entsprechenden URL auf die Benutzeroberfläche des WebShield e500 zu, und melden Sie sich an (siehe Schritt 2 auf Seite 36 bis Schritt 7 auf Seite 39).
3. Wählen Sie in der Navigationsleiste **System Maintenance (Systemverwaltung)** aus.
4. Klicken Sie neben “Save system settings“ (Systemeinstellungen speichern) auf **Save to file (In Datei speichern)**.

   Eventuell wird in Ihrem Browser ein Dialogfeld zum Herunterladen einer Datei angezeigt, um sicherzustellen, daß Sie Dateien vom WebShield e500 herunterladen möchten. Falls dieses Dialogfeld angezeigt wird, klicken Sie auf **OK** .

   Das Dialogfeld “Save As“ (Speichern unter) wird angezeigt.
5. Wählen Sie einen Speicherort für die Konfigurationsdateien und ändern Sie ggf. den Namen der .ZIP-Datei. In der Standardeinstellung lautet der Name ws_cfg_backup.zip.

6. Klicken Sie auf **Save (Speichern)**.

   Der Web-Browser erstellt die Konfigurationsdateien. Falls keine Probleme aufgetreten sind, wird ein Bestätigungsdialogfeld angezeigt.

7. Schließen Sie das Bestätigungsdialogfeld.

   Sie können jetzt die Verwaltung des WebShield e500 fortsetzen.

Wiederherstellen der Einstellungen

Stellen Sie sicher, daß beim Wiederherstellen der Geräteeinstellungen mit einer Konfigurationsdatei auch alle anderen erforderlichen Änderungen vorgenommen werden. Sie können dieselbe Konfigurationsdatei beispielsweise für mehrere Geräte verwenden. Diese Geräte können jedoch nicht dieselbe IP-Adresse verwenden (jedes Gerät muß eine eigene, eindeutige IP-Adresse erhalten), d. h., sie müssen die IP-Adressen entsprechend ändern.

Sie können zum Konfigurieren von WebShield e500 Konfigurationsdateien früherer Versionen verwenden. Wenn Sie also vor dem Aktualisieren von WebShield e500 eine solche Konfigurationsdatei erstellt haben, kann das aktualisierte Gerät Ihre Einstellungen mit Hilfe dieser Datei übernehmen.

So stellen Sie die Geräteeinstellungen aus einem Satz von Konfigurationsdateien wieder her:

1. Öffnen Sie den Webbrowser des Computers auf dem sich die Konfigurationsdateien befinden. Greifen Sie anschließend mit der entsprechenden URL auf die Benutzeroberfläche des WebShield e500 zu, und melden Sie sich an (siehe Schritt 2 auf Seite 36 bis Schritt 7 auf Seite 39).

   Wenn Sie bereits Zugriff auf die Benutzeroberfläche des Geräts haben, die Konfigurationsdateien sich aber auf einem anderen Computer befinden, übertragen Sie die Dateien auf den von Ihnen benutzten Computer.

2. Führen Sie einen der folgenden Schritte aus (die Vorgehensweise hängt davon ab, wie Sie WebShield konfigurieren möchten):

   - Wenn Sie die Gerätesoftware gerade aktualisiert haben oder das Gerät zum ersten Mal konfigurieren, enthält die Seite “System Configuration“ (Systemkonfiguration) einen extra Bereich “Restore Configuration“ (Konfiguration wiederherstellen). Klicken Sie auf der Seite “System Configuration“ (Systemkonfiguration) auf **Restore Configuration (Konfiguration wiederherstellen)**.

     ☐ **HINWEIS:** Dieser Bereich ist allerdings nur dann über **System Configuration (Systemkonfiguration)** verfügbar, wenn das Gerät zum ersten Mal konfiguriert wird.

   - Wenn Sie das Gerät zuvor schon einmal konfiguriert haben, wählen Sie in der Navigationsleiste **System Maintenance (Systemverwaltung)**, um die Seite **System Maintenance (Systemverwaltung)** aufzurufen. Achten Sie im Besonderen auf die Textfelder **File (Datei)** und **URL** neben **Restore System Settings (Systemeinstellungen wiederherstellen)**.

3. Geben Sie den vollständigen Pfad oder die vollständige URL zu den Konfigurationsdateien in das Textfeld **File (Datei)** oder **URL (URL)** ein. Beispiele:

   ```
   c:\eigenedateien\ws_cfg_backup.zip
   ```

   ```
   http://www.meinefirma.com/eigenedateien/ws_cfg_backup.zip
   ```

   Sie können auch auf **Browse (Durchsuchen)** klicken, um nach der Datei zu suchen.

4. Klicken Sie auf **Restore now (Jetzt wiederherstellen)**.

   Die Konfigurationsdateien werden im Web-Browser geöffnet und die Einstellungen an den WebShield gesendet. Sie können jetzt die Verwaltung des WebShield fortsetzen.

Wiederherstellen und Aktualisieren der Gerätesoftware

Sollte ein Problem mit einer der Festplatten des WebShield e500 auftreten, können Sie die fehlerhafte Festplatte während des Betriebs durch eine andere (mit den gleichen Spezifikationen) ersetzen. Der WebShield e500 kopiert das Image von der vorhandenen Festplatte auf die Ersatzfestplatte (siehe Seite 70).

Es können jedoch auch Umstände auftreten, bei denen Sie die Gerätesoftware auf beiden Festplatten wiederherstellen müssen. Dieser Fall ist recht unwahrscheinlich, kann aber eintreten, wenn Sie beide Festplatten gleichzeitig aus dem WebShield e500 entfernen. Für den Wiederherstellungsprozeß ist die Wiederherstellungs-CD des WebShield e500 erforderlich.

Sie haben vielleicht auch eine Aktualisierungs-CD für den WebShield e500 von Ihrem Supportvertreter erhalten, die eine verbesserte Version der Gerätesoftware enthält. Die Aktualisierung der Gerätefestplatten mit dieser CD erfolgt auf ähnliche Weise wie eine Wiederherstellung der Software.

☐ **HINWEIS:** Zum Wiederherstellen oder Aktualisieren der Software müssen Sie eine lokale Verbindung mit dem WebShield e500 herstellen. Sie können eine Wiederherstellung oder Aktualisierung nicht remote ausführen.

Beim Wiederherstellen der Gerätesoftware wird jede zusätzliche Software entfernt, die eventuell installiert worden ist. Falls Sie ePolicy Orchestrator mit dem WebShield e500 verwenden, müssen Sie den ePolicy Orchestrator-Agenten nach der Wiederherstellung neu installieren (siehe Konfigurationshandbuch).

So stellen Sie die Gerätesoftware wieder her bzw. führen eine Aktualisierung durch:

1. Schließen Sie eine Tastatur am Tastatur-Port des WebShield e500 an (purpurfarbener Port, siehe F auf Seite 17).
2. Schließen Sie einen Bildschirm am Bildschirm-Port des WebShield e500 an (siehe G auf Seite 17).
3. Falls der WebShield e500 ausgeschaltet ist, schalten Sie ihn ein.
4. Legen Sie die Wiederherstellungs- oder Aktualisierungs-CD des WebShield e500 in das CD-ROM-Laufwerk des Geräts ein (siehe B auf Seite 15). Welche CD Sie verwenden, hängt davon ab, ob die Software wiederhergestellt oder aktualisiert werden soll.

5. Drücken Sie den Reset-Schalter im Bedienfeld auf der Vorderseite des Geräts (siehe C auf Seite 16).

   Der WebShield e500 führt die Startsequenz aus. Dann wird die CD eingelesen und eine Lizenzvereinbarung angezeigt.

   ☐ **HINWEIS:** Die folgenden Schritte gelten für die WebShield e500 Wiederherstellungs-CD. Sollten jedoch andere Bildschirmaufforderungen für Ihre CD angezeigt werden, folgen Sie diesen.

   ---

6. Lesen Sie die Lizenzvereinbarung sorgfältig durch, dann geben Sie J ein, um sie zu akzeptieren.

   Falls Sie nicht mit den Bedingungen der Lizenzvereinbarung einverstanden sind, geben Sie N ein, um die Vereinbarung abzulehnen. Sie können die Software auf der CD dann nicht verwenden.

   Die folgenden Optionen werden angezeigt:

   1: Perform a full installation (Vollständige Installation ausführen) löscht alle Daten von den Festplatten des WebShield e500 und installiert die Software neu.

   2: Install software on this CD (Software auf dieser CD installieren) installiert die Software neu, während versucht wird, die folgenden Bereiche zu erhalten:

   - Konfigurationsdaten
   - Protokolldaten
   - In den Quarantänebereich verschobene E-Mail-Nachrichten
   - Zurückgestellte E-Mail-Nachrichten

   Falls der Wiederherstellungsprozeß diese Bereiche nicht erhalten kann, werden sie neu erstellt.

   3: Perform a software upgrade (Softwareaktualisierung ausführen) führt die jeweiligen Softwareaktualisierungen durch (wenn verfügbar), die auf der CD erhalten sind.

   4: Automatic operation (Automatischer Betrieb) stellt fest, welche der drei genannten Optionen am besten geeignet ist, und führt die entsprechende Option aus.

5: Perform a full installation and stop (Vollständige Installation ausführen und anhalten) löscht alle Daten von den Festplatten des WebShield e500 und installiert die Software neu. Nach der Installation wird die CD vom WebShield e500 ausgeworfen, aber es wird nicht neu gestartet. Sie können das Gerät dann abschalten.

6: Reset passwords to factory default (Kennwörter auf Werkseinstellungen zurücksetzen) setzt das Kennwort des WebShield e500 auf das Standardkennwort `e500changeme` zurück.

7: Do nothing and reboot (Nichts ausführen und neu starten) nimmt keinerlei Änderungen am WebShield e500 vor und wirft die CD aus. Sie verwenden diese Option, wenn Sie die CD versehentlich eingelegt haben und weder eine Wiederherstellung noch eine Aktualisierung der Gerätesoftware durchführen möchten.

7. Geben Sie die Nummer der gewünschten Option ein.

   Sie werden gefragt, ob die gewünschte Option weiter ausgeführt werden soll.

8. Geben Sie `J` ein.

   Der Wiederherstellungs- oder Aktualisierungsprozeß beginnt, es sei denn, Sie haben die Option **7: Do nothing and reboot (Nichts ausführen und neu starten)** gewählt. Der Fortschritt wird in einem Statusfenster angezeigt. Abhängig von der gewählten Option dauert der Prozeß bis zu 30 Minuten.

WARNUNG: Abhängig von der gewählten Option wird der WebShield e500 eventuell auf die Standardeinstellungen zurückgesetzt und alle von Ihnen vorgenommenen Konfigurationseinstellungen gehen verloren.

Nach Abschluß des Wiederherstellungs- oder Aktualisierungsprozesses wirft der WebShield e500 die CD aus und startet neu (es sei denn, Sie haben die Option **5: Perform a full installation and stop (Vollständige Installation ausführen und anhalten)** gewählt). Nach Abschluß der Startsequenz (nach etwa zwei Minuten) ist der WebShield e500 einsatzbereit. Abhängig von der gewählten Option müssen Sie eventuell die Einstellungen neu konfigurieren (siehe Seite 36).

☐ **HINWEIS:** Wenn Sie auf den WebShield e500 zugreifen und sich anmelden, denken Sie daran, daß die folgenden Änderungen eingetreten sein können, wenn Sie nicht gewählt haben, daß die vorhandenen Einstellungen erhalten werden sollen (oder wenn sie nicht erhalten werden konnten):

- Das Kennwort wurde auf das Standardkennwort `e500changeme` zurückgesetzt.
- Der LAN1-Port wurde auf die Standard-IP-Adresse 10.1.1.108 zurückgesetzt.
- Der LAN2-Port wurde aktiviert und auf die Standard-IP-Adresse 10.1.2.108 zurückgesetzt.

Informationen zu den Standardeinstellungen des WebShield finden Sie im Anhang A im Produkthandbuch.

Fehlerbehebung

Hardwarefehler

In diesem Abschnitt sind Lösungen zu Problemen enthalten, die beim Installieren und Ausführen der Anwendung auftreten können. Lösungen zu Problemen mit der Benutzeroberfläche finden Sie auf Seite 71.

Das Gerät wird nicht mit Strom versorgt

Überprüfen Sie folgendes:

- Das Gerät ist über das mitgelieferte Kabel ordnungsgemäß an eine funktionierende Steckdose angeschlossen.
- Sowohl der Stromversorgungsschalter als auch der Ein-Schalter befinden sich in EIN-Stellung (siehe Schritt 6 auf Seite 35).

  Der Netzschalter befindet sich auf der Rückseite des Geräts (siehe E auf Seite 17). Der Ein-Schalter befindet sich in dem Bedienungsfeld an der Vorderseite des Geräts (siehe C auf Seite 16).

Falls das Gerät immer noch nicht mit Strom versorgt wird, überprüfen Sie die Steckdose, indem Sie ein anderes Gerät anschließen. Funktioniert die Steckdose, liegt das Problem beim Gerät oder dem Netzkabel zum Gerät. Wenden Sie sich an Ihren Händler.

Das Gerät empfängt keine Meldungen aus meinem Netzwerk

Überprüfen Sie folgendes:

- Das Gerät ist eingeschaltet und die Software wird ausgeführt; dies wird durch die leuchtende LED der Stromversorgungsanzeige angezeigt (im Bedienungsfeld, siehe C auf Seite 16). Die LEDs für das Festplattenlaufwerk leuchten nicht (siehe A auf Seite 15).
- Das verwendete Netzwerkkabel ist unbeschädigt und ordnungsgemäß an den Daten-Port des Geräts und die vorhandenen Netzwerkkomponenten angeschlossen. Falls Sie nicht die mit dem Gerät gelieferten blauen Kabel verwendet haben, stellen Sie sicher, daß die Kabel durchgängige (ungekreuzte) UTP-Netzwerkkabel der Kategorie 5 sind.
- Wenn Sie WebShield im Transparenzmodus betreiben, muß das Gerät über den LAN2-Port mit den vorhandenen Netzwerkkomponenten verbunden sein.

Falls das Gerät immer noch keinen Netzwerkverkehr empfängt, überprüfen Sie die Netzwerkkabel und die Netzwerk-Ports an den vorhandenen Netzwerkgeräten. Funktionieren Kabel und Ports ordnungsgemäß, liegt das Problem beim Gerät. Wenden Sie sich an Ihren Händler.

Eine LED des Festplattenlaufwerks leuchtet rot

Das Festplattenlaufwerk ist fehlerhaft und muß ersetzt werden.

Die Laufwerke sind in Caddies untergebracht, so daß Sie ein fehlerhaftes Laufwerk ersetzen können, während das Gerät in Betrieb ist. Das Ersatzlaufwerk wird automatisch von dem vorhandenen Laufwerk aus abgebildet.

WARNUNG: Beachten Sie beim Ersetzen von Festplattenlaufwerken unbedingt folgende Punkte:

- Entfernen Sie nie beide Laufwerke gleichzeitig aus dem Gerät. Mindestens ein Laufwerk muß immer im Gerät bleiben.
- Achten Sie darauf, das Gerät nicht länger als ein paar Minuten mit nur einem Laufwerk zu betreiben, da dies den Luftstrom verändert und zu einer Überhitzung des Geräts führen kann. Setzen Sie das Ersatz-Laufwerk sofort ein.
- Verwenden Sie nur Laufwerke mit genau derselben Spezifikation wie die vorhandenen Laufwerke.
- Achten Sie bei der Handhabung der Laufwerke darauf, keine Bauteile zu berühren, die empfindlich auf statische Ladung reagieren. Halten Sie die üblichen Vorkehrungen zur Vermeidung statischer Aufladung ein, und berühren Sie nicht mit Ihrer Hand oder einem anderen Objekt das Innere des leeren Laufwerkspalts des Geräts.

So ersetzen Sie ein fehlerhaftes Laufwerk:

1. Drücken Sie auf die Entriegelungstaste des fehlerhaften Laufwerks, und ziehen Sie dann den Griff nach unten (Abbildung 2-5). Ziehen Sie das Laufwerk aus dem Laufwerkspalt.

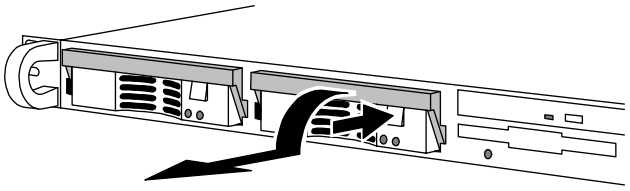


Abbildung 2-5. Entfernen des Laufwerks

2. Führen Sie das Ersatzlaufwerk in den leeren Laufwerkspalt ein, und drücken Sie dessen Griff nach oben, um das Laufwerk in dieser Position zu verriegeln (Abbildung 2-6).

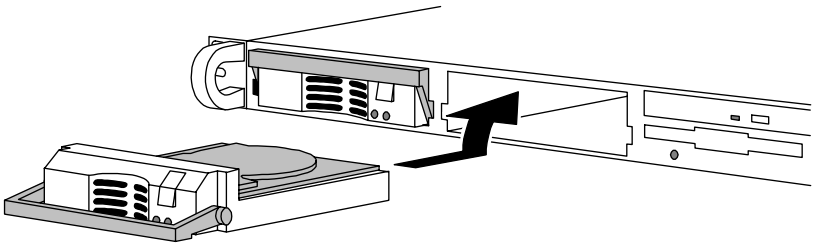


Abbildung 2-6. Einsetzen des Laufwerks

Das Gerät kopiert das Image von dem vorhandenen Laufwerk auf das Ersatzlaufwerk. Dies kann 20–30 Minuten dauern. In dieser Zeit blinkt die grüne LED des Ersatzlaufwerks.

Beide LEDs des Festplattenlaufwerks leuchten rot

Bei den Laufwerken des Geräts liegt ein Problem vor. Verwenden Sie die WebShield e500-Wiederherstellungs-CD, um die Software auf dem Gerät wiederherzustellen (siehe Seite 64). Falls Sie damit keinen Erfolg haben, wenden Sie sich an Ihren Händler.

Probleme mit der Benutzeroberfläche

In diesem Abschnitt sind Lösungen zu Problemen enthalten, die beim Konfigurieren des Geräts über die Benutzeroberfläche auftreten können.

Sie können nicht auf die Seite “Log on“ (Anmeldung) zugreifen

Überprüfen Sie folgendes:

- Das Gerät ist eingeschaltet und die Software wird ausgeführt; dies wird durch die leuchtende LED der Stromversorgungsanzeige angezeigt (im Bedienungsfeld, siehe C auf Seite 16). Die LEDs für das Festplattenlaufwerk leuchten nicht (siehe A auf Seite 15).
- Sie haben in dem URL-Feld Ihres Web-Browsers `https` (nicht `http`) verwendet. Stellen Sie sicher, daß Ihr Browser SSL (Secure Sockets Layer) v3.0-Verschlüsselung unterstützt, und daß diese aktiviert ist.
- Auf dem Verwaltungscomputer (dem Computer, mit dem Sie das Gerät verwalten) ist das Gerät nicht als dessen Proxy konfiguriert. Falls Sie zwischen dem Verwaltungscomputer und dem Gerät einen Proxy haben, muß das Gerät als Übergabe-Host des Proxy konfiguriert werden.
- Falls Sie über den LAN1-Port eine Remote-Verbindung zu dem Gerät über das Netzwerk haben (siehe H auf Seite 18), stellen Sie folgende Punkte sicher:
  - Der verwendete Computer hat eine funktionstüchtige Verbindung zu Ihrem Netzwerk und kann dasselbe Subnet erreichen, mit dem auch das Gerät verbunden ist.
  - Sie haben in dem URL-Feld Ihres Web-Browsers die neue IP-Adresse verwendet, die Sie für den LAN1-Port konfiguriert haben. Falls Sie die standardmäßige IP-Adresse `10.1.1.108` nicht deaktiviert oder gelöscht haben, versuchen Sie es mit dieser IP-Adresse (`https://10.1.1.108`).

    Die IP-Adresse des Geräts muß für das Subnet geeignet sein, mit dem das Gerät verbunden ist. Ist sie nicht geeignet, versuchen Sie es mit der standardmäßigen IP-Adresse. Führt dies ebenfalls nicht zum Erfolg, versuchen Sie es über eine direkte Verwaltungsverbindung (siehe Schritt 4 auf Seite 33).

    ☐ **HINWEIS:** Über den LAN2-Port erhalten Sie nur eine direkte Verwaltungsverbindung, wenn Sie das Gerät im Proxymodus verwenden , *und* wenn Sie den LAN2-Port (Schritt 17 auf Seite 41) nicht deaktiviert haben.

  - Das Gerät hat eine funktionierende Verbindung zu Ihrem vorhandenen Netzwerk, die durch die blinkende NIC 1 LED für Netzwerkaktivität angezeigt wird (im Bedienungsfeld, siehe C auf Seite 16).

    Blinken die LEDs nicht, stellen Sie sicher, daß das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN1-Port des Geräts und an Ihre vorhandenen Netzwerkgeräte angeschlossen ist. Falls Sie nicht das mit dem Gerät gelieferte blaue Kabel verwendet haben, stellen Sie sicher, daß das Kabel ein durchgängiges (ungekreuztes) UTP-Netzwerkkabel der Kategorie 5 ist.

- Wenn das Gerät im Proxy-Modus arbeitet und Sie eine direkte lokale Verwaltungsverbindung über den LAN2-Port haben (siehe I auf Seite 19), stellen Sie folgende Punkte sicher:

  - Sie haben den LAN2-Port nicht deaktiviert. Sie müssen eine Remote-Verbindung herstellen, um dies überprüfen zu können.

  - Sie haben in das URL-Feld Ihres Web-Browsers die neue IP-Adresse eingegeben, die Sie für den LAN2-Port konfiguriert haben (die standardmäßige IP-Adresse lautet `10.1.2.108`).

  - Das Gerät hat eine funktionierende Verbindung zu Ihrem Computer, die durch die blinkende NIC 2 LED für Netzwerkaktivität angezeigt wird (im Bedienungsfeld, siehe C on Seite 16).

    Blinkt die LED nicht, stellen Sie sicher, daß das verwendete Kabel unbeschädigt und ordnungsgemäß an den LAN2-Port des Geräts und an den Netzwerk-Port Ihres Computers angeschlossen ist. Falls Sie nicht das mit dem Gerät gelieferte, orangefarbene Kabel verwendet haben, stellen Sie sicher, daß das Kabel ein gekreuztes UTP-Netzwerkkabel der Kategorie 5 ist.

Die Seite Log on (Anmelden) wird angezeigt, doch die Schaltfläche Log on (Anmelden) trägt die Beschriftung Initializing (Initialisierung)

Das Gerät überprüft Ihren Web-Browser auf die Komponenten, die für die Benutzeroberfläche erforderlich sind.

Das Gerät wurde für Internet Explorer v4.0, v5.0, v5.5 oder v5.5 optimiert und unterstützt Netscape Navigator v4.7. Falls Sie einen anderen Web-Browser verwenden, können Sie u. U. nicht auf die Benutzeroberfläche zugreifen und das Gerät nicht konfigurieren.

Die Benutzeroberfläche des Geräts benötigt die Java 2-Laufzeitumgebung, so daß Ihr Browser diese Software möglicherweise erst installieren muß. Die Größe der Java 2-Laufzeitumgebung beträgt (je nach den für Ihren Browser erforderlichen Komponenten) 5–14MB. Die Installation kann länger dauern, falls Sie eine langsame Datenverbindung zu dem Gerät haben.

Ihr Kennwort funktioniert nicht

Falls Sie kürzlich die Software des Geräts wiederhergestellt haben, ohne die vorherigen Einstellungen beizubehalten, wird das Kennwort auf das Standardkennwort `e500changeme` zurückgesetzt.

Sie haben ihr Kennwort vergessen

Verwenden Sie die WebShield e500-Wiederherstellungs-CD, um das Kennwort des Geräts auf das Standardkennwort `e500changeme` zurückzusetzen (siehe “Wiederherstellen und Aktualisieren der Gerätesoftware“ auf Seite 64). Verwenden Sie die Option **6: Reset passwords to factory default (Kennwörter bei der Wiederherstellung auf werkseitige Einstellung zurücksetzen)**.

Ein Teil der Benutzeroberfläche wird nicht ordnungsgemäß angezeigt

Die Benutzeroberfläche des Geräts wurde für Internet Explorer v4.0, v5.0, v5.5 oder v6.0 optimiert und unterstützt Netscape Navigator v4.7. Überprüfen Sie die beigefügten Versionsinformationen, um herauszufinden, ob es bei der Verwendung einiger Web-Browser auf bestimmten Betriebssystemen Probleme gibt.

Ihre Clients (Software) können nicht über das Gerät kommunizieren

Überprüfen Sie folgendes:

- Die für das Gerät erforderlichen Proxys sind aktiviert (standardmäßig sind alle unterstützten Protokolle aktiviert, siehe “Konfigurieren der Protokolle des WebShield e500“ auf Seite 46).
- Die Clients und andere Geräte sind so konfiguriert, daß sie den Datenverkehr an das und von dem Gerät leiten (siehe “Konfigurieren weiterer Geräte“ auf Seite 53).
- Es liegen keine Netzwerkprobleme vor, und Ihre Geräte sind ordnungsgemäß angeschlossen.

Das Surfen im Internet ist nicht möglich oder die Blockierung der URL ist nicht durchgesetzt

Das Gerät muß Zugriff auf einen DNS-Server haben, um Web-Browsing (HTTP)-Anfragen zu überprüfen und zu ermitteln, welche URLs blockiert werden sollen, falls das Blockieren von URLs konfiguriert ist. Daher müssen Sie auf der Seite “System Configuration“ (Systemkonfiguration) einen DNS-Server konfigurieren (siehe Schritt 9 auf Seite 39).

Guide d'installation – Français

Présentation

Ce Guide d'installation contient les informations d'installation et de configuration de l'application WebShield. Veuillez consulter les sections suivantes pour obtenir des informations spécifiques:

Copyright et attribution de marques commerciales **Page 2**

Informations sur l'alimentation et la sécurité **Page 3**

A propos de l'application WebShield e500 **Page 5**

- Fonctionnalités Page 6
- Contenu fourni avec l'application Page 10

Mise en route de l'application **Page 13**

- Installateur de l'application Page 13
- Ports et connecteurs Page 14
- Collecter les informations de configuration Page 19

Installation de l'application **Page 31**

Configuration des paramètres réseau **Page 35**

Configuration des paramètres de protocole **Page 45**

- Configuration des protocoles de l'application Page 46
- Configuration de la fonctionnalité de mise à jour automatique Page 52
- Configuration des autres équipements Page 53
- Tester votre configuration Page 55

Utilisation de l'application **Page 59**

- Sauvegarde et restauration de vos paramètres Page 61
- Restauration et mise à niveau du logiciel de l'application Page 63

Dépannage **Page 67**

- Problèmes matériels Page 67
- Problèmes d'interface utilisateur Page 70

Copyright et attribution de marques commerciales

COPYRIGHT
© 2001–2002 Networks Associates Technology, Inc. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, transmise, transcrite, stockée dans un système de recherche ou traduite dans toute autre langue sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite de Networks Associates Technology, Inc., ou de ses fournisseurs ou filiales. Pour obtenir cette autorisation, écrivez au service juridique de Network Associates à l'adresse suivante: 3965 Freedom Circle, Santa Clara, California 95054, ou appelez le +1-972-308-9960.

MARQUES DÉPOSÉES

Active Security, Active Security (en katakana), ActiveHelp, ActiveShield, AntiVirus Anyware (et conception), Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert (et conception), CyberCop, CyberCop (en katakana), CyberMedia, CyberMedia UnInstaller, Design (N stylisé), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (en katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (en katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (en katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, ISDN TEL/SCOPE, LANGuru, LANGuru (en katakana), M (et conception), Magic Solutions, Magic Solutions (en katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (en katakana), McAfee (et conception), MultiMedia Cloaking, Net Tools, Net Tools (en katakana), NetCrypto, NetOctupus, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PC Medic 97, PCNotary, PGP, PGP (Pretty Good Privacy), Pretty Good Privacy, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, RingFence, Router PM, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (dans En Hangul), SniffMaster, SniffMaster (dans En Hangul), SniffMaster (en katakana), SniffNet, Stalker, SupportMagic, TIS, TMEG, TNV, TVD, TNS, Total Network Security, Total Network Visibility, Total Network Visibility (en katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (en katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager sont des marques déposées de Network Associates, Inc. et/ou de ses filiales aux Etats-Unis et/ou dans d'autres pays. Toutes les autres marques, déposées ou non, de ce document appartiennent uniquement à leurs propriétaires respectifs.

CONTRAT DE LICENCE

A L'ATTENTION DE TOUS LES UTILISATEURS: Lisez attentivement le contrat correspondant à la licence que vous avez achetée. Il définit les termes et les conditions générales relatifs à l'utilisation du logiciel sous licence. Si vous ne CONNAISSEZ PAS LE type de licence vous avez acquis, consultez les documents de vente, d'attribution de licence ou le bon de commande, qui accompagnent le logiciel ou que vous avez reçus séparément lors de l'achat (sous la forme d'un livret, d'un fichier sur le CD-ROM du produit ou d'un fichier disponible sur le site Web à partir duquel vous avez téléchargé le package logiciel). SI VOUS NE SOUSCRIVEZ PAS A TOUS LES TERMES DU PRESENT CONTRAT, N'INSTALLEZ PAS LE LOGICIEL. SI CELA EST POSSIBLE, VOUS POUVEZ RETOURNER LE PRODUIT A NETWORKS ASSOCIATES OU LA OU VOUS L'AVEZ ACHETE. VOUS SEREZ REMBOURSE INTEGRALEMENT.

Informations sur l'alimentation et la sécurité

IMPORTANT : Pour garantir le fonctionnement en toute sécurité de l'application WebShield e500, lisez attentivement toutes les informations suivantes *avant* d'installer l'application.

Configuration requise de l'alimentation

- Vérifiez la compatibilité du cordon d'alimentation dans le pays d'utilisation. En cas de non conformité, contactez votre fournisseur. N'essayez en aucun cas de modifier vous-même le cordon d'alimentation.
- La prise électrique à laquelle vous connectez l'application doit être strictement conforme aux standards électriques du pays d'utilisation.
- Lorsque vous branchez l'application à la source électrique ou à un autre appareil, assurez-vous que les câbles sont rangés ou regroupés en toute sécurité et qu'ils ne présentent ainsi aucun danger.

Utilisation de l'application

- N'ouvrez pas le boîtier de l'application. Il ne s'y trouve aucun élément utilisable.
- L'application est lourde. Quand vous soulevez le matériel, tenez-le fermement afin de ne pas vous blesser ou d'endommager l'application.
- Placez le matériel sur une surface plate et résistante, comme un bureau, ou placez-le à l'abri dans un rack, comme un rack 19 pouces. Assurez-vous que la surface ou le rack supporte le poids du matériel, et que celui-ci est stable et ne risque aucunement de tomber.
- Ne placez aucun objet lourd sur l'application.
- Les ports réseau du matériel ne doivent être utilisés qu'avec des connecteurs RJ-45. Ne pas les utiliser avec du matériel téléphonique, sauf si la prise en question est conçue spécialement pour une utilisation Ethernet 10 Mbits/s ou 100 Mbits/s.
- Au cas peu probable où l'équipement subirait une défaillance matérielle, mettez l'application hors tension et débranchez-la de la prise d'alimentation. Contactez votre fournisseur.

Conditions de fonctionnement

- Vérifiez que l'environnement autour de l'application garantit une utilisation informatique normale. Assurez-vous de l'absence d'humidité et de la présence d'une ventilation appropriée. La température de fonctionnement doit être comprise entre 10 et 40°C, et le taux d'humidité entre 0 et 90 %. En cas de non-respect de ces valeurs, le bon fonctionnement de l'application n'est plus garanti.
- Assurez-vous également qu'il existe un espace d'au moins 25 mm à l'arrière du matériel, de telle sorte que le rafraîchissement automatique de l'application se déroule correctement.
- Veillez à ce qu'aucun liquide ou objet ne passe à travers les orifices de ventilation ou la grille d'aération.

A propos de l'application WebShield e500

L'application WebShield e500 (Figure 3-1) est un serveur spécialisé d'analyse et de gestion de contenu doté du puissant logiciel WebShield. Elle est entièrement configurable via un navigateur Web et peut être utilisée dans pratiquement toutes les topologies de réseau. Elle fournit une analyse des virus pour les protocoles suivants:

- Messages électroniques SMTP (Simple Mail Transfer Protocol)
- Echanges FTP (File Transfer Protocol)
- Navigation Web HTTP (Hypertext Transfer Protocol)
- Messages électroniques Internet POP3 (Post Office Protocol version 3)

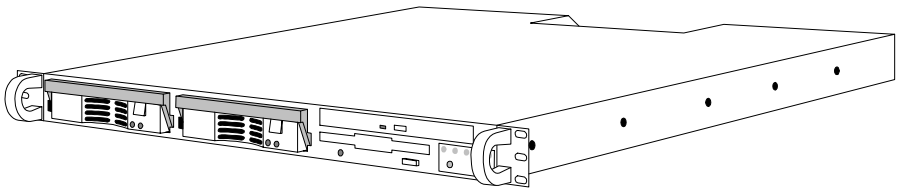


Figure 3-1. Application WebShield e500

Grâce à des fonctionnalités supplémentaires telles que l'analyse de contenu, la protection anti-relais et anti-spam, l'application offre une protection complète pour votre passerelle Internet, empêchant tout matériel indésirable d'entrer ou de quitter votre entreprise.

L'application WebShield e500 partage ses ressources entre les protocoles qu'elle analyse, vérifiant le trafic entrant et sortant selon les besoins. Elle peut détecter, nettoyer, consigner et mettre en quarantaine des éléments de courrier électronique infectés, y compris des fichiers et macros compressés, les empêchant d'atteindre leurs destinataires prévus. Elle peut également bloquer des éléments HTTP, FTP et POP3 infectés.

L'utilisation de l'application pour effectuer les analyses de détection des virus permet à votre serveur de messagerie de se consacrer entièrement aux activités de courrier. Vous pouvez aussi utiliser conjointement plusieurs applications WebShield e500 afin d'accroître le débit d'analyse et de fournir une fonction de tolérance de pannes.

Pour plus d'informations sur les différentes façons d'utiliser l'application ou pour obtenir quelques exemples de topologie, reportez-vous au chapitre 1 du Guide produit.

Fonctionnalités

Transparence — nouvelle fonctionnalité de la version 2.5

Si vous avez déjà utilisé une précédente version de l'application WebShield, sachez que la version 2.5 propose une nouvelle fonctionnalité, la transparence. Cela signifie que vous pouvez désormais utiliser l'application en *mode proxy* ou en *mode transparence*:

- **Mode proxy** (proxy explicite): convient aux réseaux dans lesquels l'équipement peut être aisément configuré pour acheminer le trafic via l'application. Avant l'ajout de la fonction de transparence, l'application ne fonctionnait qu'en mode proxy.

  En mode proxy, l'application gère uniquement le trafic des protocoles pour lesquels elle fait office de proxy.

- **Mode transparence** (proxy transparent): permet d'intégrer l'application dans les réseaux où la reconfiguration d'un autre matériel constitue une opération longue ou difficile. L'application repose alors de façon transparente sur le réseau et utilise les informations de routage statiques et dynamiques pour recevoir et transmettre le trafic analysé.

  ❑ **REMARQUE :** En mode transparence, l'application doit être connectée à deux sous-réseaux différents (via les ports réseau local 1 et réseau local 2).

  L'application gère la totalité du trafic IP entre les deux sous-réseaux.

Pour plus d'informations sur ces modes, consultez la section « Proxy ou transparence ? » du Guide produit.

IMPORTANT : Comme les deux modes sont différents, il importe que vous sachiez lequel vous voulez utiliser *avant* d'installer l'application et de la configurer.

Pour plus d'informations sur la configuration de l'application avec un fichier de configuration provenant d'une version précédente de l'application, voir "Restauration de vos paramètres" à la page 62.

Quelques autres fonctionnalités de l'application sont résumées dans le reste de la présente section.

Matériel

L'application possède de nombreuses fonctionnalités, dont notamment:

- Plate-forme serveur 1U à monter en rack de 19 pouces.
- Double processeur Intel Pentium III de 1GHz.
- 256Mo de mémoire SDRAM PC 133 MHz.
- Deux ports réseau Ethernet RJ-45 10/100 Mbits/s à détection automatique, assurant la flexibilité des connexions au réseau existant et une interface de gestion dédiée (disponible uniquement en mode proxy).
- Deux unités de disque dur SCSI 17,4 Go « connectables à chaud » gérées dans une configuration matérielle RAID 1 (miroir). Cette configuration garantit un traitement transparent dans l'éventualité peu probable d'un problème sur l'une des unités. Lorsque vous insérez une unité de remplacement, le contrôleur RAID reflète automatiquement la nouvelle unité.

Pour plus d'informations sur les ports et connecteurs de l'application, voir page 14.

Logiciel

Le logiciel de l'application offre les fonctionnalités suivantes:

- Gestion Web par cryptage SSL (Secure Sockets Layer) à partir d'un navigateur Web.
- Une interface utilisateur simple à configurer, afin de vous permettre de rapidement configurer l'application. L'application nécessite alors un minimum d'intervention de la part de l'utilisateur.
- Des serveurs proxy simples à configurer, et ce même dans des environnements complexes; voir “Collecter les informations de configuration” à la page 19.
- Analyse des virus pour les messages électroniques SMTP, vérification des éléments infectés et du contenu interdit. Les autres fonctionnalités SMTP incluent:
  - Des configurations de remise de courrier SMTP souples, qui vous permettent de configurer plusieurs méthodes de remise de courrier et d'introduire des fonctions de tolérance de pannes.
  - Analyse de contenu souple des messages, qui vous permet de rechercher du contenu interdit et de bloquer des types de pièces jointes spécifiques.

  - Blocage du spam (rejet des messages électroniques non sollicités) par le destinataire, l'expéditeur ou le serveur.
  - Prise en charge des listes Blackhole en temps réel, permettant d'identifier des sources potentielles de messages spam. L'application peut utiliser ces listes pour bloquer les messages non sollicités. Des listes Blackhole sont disponibles auprès de nombreuses organisations, notamment la MAPS (Mail Abuse Prevention System); voir http://www.mailabuse.org.
  - Relais de messages d'un serveur ou un nom de domaine spécifié vers un autre serveur. Il existe également une fonctionnalité anti-relais permettant d'empêcher les expéditeurs non autorisés d'utiliser l'application comme relais pour envoyer des messages électroniques non sollicités.

- Analyse des virus des échanges FTP pour des éléments infectés.
- Analyse des virus de navigation Web HTTP, blocage du contenu infecté. Vous pouvez également bloquer des messages Java, ActiveX et de script.
- Analyse des virus des messages électroniques POP3, vérification des éléments infectés.
- Analyse distincte des trafics entrant et sortant, ce qui permet de configurer différentes options d'analyse pour chaque direction.
- Des plannings de mise à jour automatique distincts pour les fichiers de définition de virus McAfee (.DAT) et le moteur d'analyse McAfee, vous garantissant une analyse des virus constamment à jour.
- Détection des virus dans des formats de fichier compressé courants.
- Actions d'analyse souples vous permettant de nettoyer, supprimer, bloquer ou mettre en quarantaine (isoler) des éléments infectés.
- Stockage de quarantaine distinct, vous permettant d'inspecter les types de messages électroniques mis en quarantaine suivants:
  - Messages entrants contenant des éléments infectés.
  - Messages sortants contenant des éléments infectés.
  - Messages entrants contenant un contenu interdit.
  - Messages sortants contenant un contenu interdit.

- Notification concernant la détection d'un élément infecté, à l'aide d'un ensemble de méthodes d'alerte configurables, telles que l'envoi d'un message électronique, la consignation au format XML, la création de rapports SNMP et la création de rapports ePolicy Orchestrator ; voir le Guide de configuration.
- La journalisation avancée des activités d'analyse et des flux de protocoles vous permettent d'afficher les performances passées et des informations de remise du courrier. Vous pouvez également générer des graphiques, des rapports et des journaux à partir de l'interface utilisateur.
- Prise en charge de McAfee ePolicy Orchestrator, qui vous permet d'intégrer l'application à un serveur ePolicy Orchestrator afin de produire des rapports statistiques, historiques, de gestion et graphiques avancés à partir des informations enregistrées par l'application; voir le Guide de configuration.
- Processus de sauvegarde rapide, qui permet de stocker et de restaurer rapidement les paramètres de l'application via le réseau; voir page 61.
- Processus de restauration rapide, qui permet de restaurer le logiciel de l'application dans l'éventualité peu probable d'un problème; voir page 63.

Ce que l'application ne fait pas

L'application offre de nombreuses fonctionnalités, mais n'oubliez pas ceci:

- Il ne s'agit *pas* d'un pare-feu. Vous devez l'utiliser au sein de votre entreprise, derrière le pare-feu existant.
- Ce n'est *pas* un serveur de messagerie. Vous devez configurer le pare-feu, le serveur de messagerie, le cache Web et les autres équipements pour acheminer le trafic via l'application; voir page 53.
- Ce n'est *pas* un agent de transfert de courrier, elle ne conserve pas de copie des messages électroniques qui la traversent, à moins que ces messages ne soient mis en quarantaine ou différés.
- Ce n'est *pas* un serveur Web d'utilité générale destiné au stockage de pages Web.
- Ce n'est *pas* un serveur d'utilité générale destiné au stockage de logiciels et fichiers supplémentaires. N'installez pas de logiciel sur l'application et n'ajoutez pas de fichier supplémentaire à moins que la documentation de l'application ou le représentant du support technique ne l'ait expressément indiqué.
- En mode proxy, elle gère uniquement le trafic SMTP, FTP, HTTP et POP3. Vous ne*devez*pas essayer d'acheminer d'autre trafic via l'application.

Contenu fourni avec l'application

Vérifiez que tous les éléments qui accompagnent l'application ont bien été livrés, contrôlez l'emballage du produit pour voir si vous n'avez pas oublié un compartiment. Si un élément est absent ou endommagé, contactez votre fournisseur.

Matériel et logiciel

- Trois câbles réseau UTP Cat 5 (catégorie 5) avec des connecteurs RJ-45:
  - Les deux câbles de couleur bleue sont des câbles droits (non croisés).
  - Le câble orange est croisé.

  "Installation de l'application" à la page 31 explique comment utiliser ces câbles avec l'application.
- Kit de montage, pour installer l'application dans un rack 19 pouces.
- CD-ROM de récupération de l'application WebShield e500.
- Différents cordons d'alimentation pour différents pays.

> **IMPORTANT :** Vérifiez la compatibilité du cordon d'alimentation dans le pays d'utilisation. Si aucun cordon compatible n'est fourni, contactez votre fournisseur. Ne branche.z pas l'application sur une source de courant avant d'avoir lu la section "Informations sur l'alimentation et la sécurité" à la page 3.

Documentation utilisateur

Ce guide est l'un des documents fournis avec l'application afin de vous aider à utiliser efficacement ce produit. Pour une description des autres documents, voir les Notes de mise à jour.

Documentation supplémentaire

- Informations de garantie et carte à retourner.
- Informations McAfee PrimeSupport.
- Informations supplémentaires, telles que des offres spéciales et des licences de parties tierces.

Eléments supplémentaires nécessaires

Vous pouvez utiliser le kit de montage pour installer l'application WebShield e500 dans un rack 19 pouces. Pour l'installer à un autre emplacement, vous aurez peut-être besoin d'équipement supplémentaire afin de préparer l'emplacement et de maintenir l'application en place. Veillez à toujours respecter les avertissements de sécurité; voir “Informations sur l'alimentation et la sécurité” à la page 3.

Pour configurer et gérer l'application, vous devez disposer d'un ordinateur connecté au même réseau que l'application ou à l'application elle-même; voir Etape 4 à la page 32. Vous pouvez alors utiliser le navigateur Web de l'ordinateur pour accéder à l'interface utilisateur de l'application.

Configuration requise pour l'ordinateur

L'interface utilisateur de l'application est optimisée pour Microsoft Internet Explorer version 4.0, 5.0, 5.5 ou 6.0, et prend en charge Netscape Navigator version 4.7.

Lorsque vous accédez à l'application, celle-ci vérifie que votre navigateur Web dispose des composants appropriés et affiche une boîte de dialogue pour tout composant absent.

Les options suivantes doivent être activées sur votre navigateur Web:

- Cryptage SSL (Secure Sockets Layer) version 3.0
- JavaScript
- ActiveX (pour Microsoft Internet Explorer)
- Plug-ins (pour Netscape Navigator)

L'affichage de l'interface utilisateur est optimal avec les paramètres d'affichage suivants:

- 65 536 couleurs (256 couleurs minimum)

- Résolution 1152 x 864

Restauration ou mise à niveau du logiciel de l'application

Outre la gestion générale de l'application, vous aurez peut-être besoin d'effectuer les opérations suivantes:

- Restauration du logiciel de l'application sur les deux unités de l'application, dans l'éventualité peu probable d'un problème.
- Mise à niveau du logiciel de l'application à l'aide d'un CD-ROM de mise à niveau de l'application WebShield e500.

Pour effectuer ces tâches, vous devez connecter un clavier et un moniteur directement à l'application; pour plus d'informations, voir page 63.

Mise à jour des fichiers de définition de virus (.DAT) et du moteur d'analyse de l'application

La fonctionnalité de mise à jour automatique de l'application maintient le fichier.DAT et le moteur d'analyse à jour, garantissant une parfaite protection contre les virus. Cette fonctionnalité est configurée via l'interface utilisateur de l'application (à l'aide du navigateur Web); voir page 52. Vous pouvez également lancer des mises à jour immédiates à tout moment, en utilisant les mêmes pages de l'interface utilisateur.

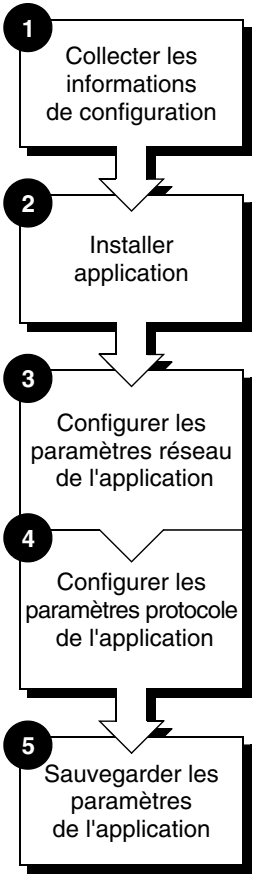
Installation des service packs et des correctifs

Vous recevrez peut-être des service packs et des correctifs du représentant du support technique, contenant des améliorations logicielles pour l'application. Si tel est le cas, vous pouvez les installer via l'interface utilisateur de l'application (à l'aide du navigateur Web). Pour plus d'informations sur les service packs et les correctifs, reportez-vous aux informations qui les accompagnent.

Mise en route de l'application

Une fois que vous avez décidé de la façon d'utiliser l'application — voir le chapitre 1 du Guide produit — vous devez effectuer les actions suivantes afin d'intégrer l'application WebShield à votre réseau actuel:

1. Collecter les informations de configuration requises; voir page 19.
2. Installer l'application à l'emplacement requis et effectuer les connexions nécessaires; voir page 31.
3. Configurer les paramètres réseau de l'application; voir page 35.
4. Configurer les paramètres de protocole de l'application; voir page 45.
5. Sauvegarder vos paramètres de façon à pouvoir rapidement reconfigurer l'application si vous devez restaurer ses unités; voir page 61.



Une fois que vous avez installé et configuré l'application, accédez à l'interface utilisateur afin de personnaliser les fonctionnalités dont vous avez besoin. Pour plus d'informations sur la configuration d'une fonctionnalité dans l'interface utilisateur, affichez la rubrique d'aide correspondante en cliquant sur le bouton d'aide ?; voir page 59.

Installateur de l'application

Nous recommandons que l'installation et la configuration de l'application soient effectuées par l'administrateur en technologie informatique responsable du système de messagerie et des passerelles Internet de votre entreprise. Le processus de configuration nécessite des informations pour les protocoles à analyser, et il doit être configuré correctement. De plus, il se peut que vous ayez à configurer d'autres équipements pour acheminer le trafic vers l'application, en fonction du mode utilisé par celle-ci (mode proxy ou mode transparent).

Pour un récapitulatif des informations requises, voir page 19.

Ports et connecteurs

Les ports et connecteurs de l'application sont présentés page vii. Les étapes de l'installation page 31 expliquent comment connecter l'équipement aux ports.

❑ **REMARQUE :** L'aspect physique de l'application peut avoir été modifiée en cours de développement. C'est pourquoi les emplacements et types des ports et connecteurs de votre application peuvent être différents de ceux figurant dans le présent guide. Si les modifications sont importantes, reportez-vous aux notes de versions ci-jointes pour des informations récentes.

Ces ports et connecteurs sont décrits ci-après.

A Deux unités de disque dur

Les deux unités sont des unités de disque dur SCSI 17,4 Go « connectables à chaud » gérées dans une configuration RAID 1 (miroir). Elles reflètent le système d'exploitation et le traitement des données de l'application, assurant un fonctionnement transparent dans l'éventualité peu probable d'un problème avec l'une des unités (signalé par un voyant rouge sur l'unité). Les unités se trouvent sur des chargeurs, ce qui permet de remplacer une unité défaillante alors que l'application fonctionne. L'image de l'unité de remplacement est automatiquement créée à partir de l'unité existante; voir “Le voyant d'une unité de disque dur est rouge” à la page 68.

B Unité de CD-ROM

L'unité de CD-ROM est utilisée pour restaurer et mettre à niveau le logiciel de l'application; elle ne doit pas être utilisée pour d'autres opérations; voir Etape 4 à la page 64.

C Panneau de contrôle

Le panneau de contrôle, situé dans le coin inférieur droit de l'application, comporte des voyants qui fournissent des informations sur le système. Il comporte également un bouton de réinitialisation et un bouton de marche/arrêt:

Bouton de réinitialisation
Redémarre l'application comme si celle-ci avait été mise hors tension puis sous tension.

Bouton de marche/arrêt
Met l'application sous tension pour qu'elle soit opérationnelle (le voyant d'alimentation est allumé). Si le bouton de marche/arrêt est relâché, l'application est en mode attente.

Lorsque l'application est en mode attente, ses ports réseau restent actifs mais aucun protocole ou donnée destiné à l'application ne peut la traverser, ce qui garantit la protection antivirus de votre entreprise.

REMARQUE : Si l'interrupteur d'alimentation électrique E (à l'arrière de l'application) est en position d'arrêt, l'application ne reçoit pas de courant; voir.

Voyant de surchauffe
S'allume lorsque l'application a trop chauffé. Ceci peut être dû à une mauvaise circulation d'air autour de l'unité, ou à une température ambiante excessive dépassant les conditions de fonctionnement normal. Ecoutez le bruit du ventilateur de l'application — situé au centre de l'unité — afin de vérifier que celui-ci est bien en état de marche. S'il ne fonctionne pas, mettez l'application hors tension et contactez votre fournisseur.

Voyants d'activité réseau
Clignotent pour signaler une activité réseau sur les ports réseau: La carte réseau 1 correspond au port LAN1 et la carte réseau 2 au port LAN2. Si ces voyants clignotent alors que le voyant d'alimentation est éteint, l'application est en mode attente.

Voyant d'activité de l'unité de CD-ROM
Clignote lorsque l'application accède au CD qui se trouve dans l'unité de CD-ROM.

Voyant d'alimentation
S'allume lorsque l'application est à la fois sous tension et opérationnelle.

D Prise d'alimentation

Utilisez le cordon d'alimentation fourni pour raccorder l'application à une prise de courant.

IMPORTANT : Vérifiez la compatibilité du cordon d'alimentation dans le pays d'utilisation. S'il ne convient pas, contactez votre fournisseur.

E Interrupteur d'alimentation électrique

Utilisez cet interrupteur pour mettre l'application sous tension afin qu'elle puisse recevoir le courant provenant de la prise de courant.

REMARQUE : Si l'interrupteur d'alimentation électrique est en position de marche mais que le bouton de marche/arrêt (sur le panneau de contrôle C à l'avant de l'application) est en position d'arrêt, l'application est en mode attente.

F Port clavier

Connectez un clavier à ce port (de couleur violette) uniquement si vous voulez restaurer ou mettre à niveau le logiciel de l'application; voir Etape 1 à la page 64.

G Port écran

Connectez un écran à ce port uniquement si vous voulez restaurer ou mettre à niveau le logiciel de l'application; voir Etape 2 à la page 64.

H Port réseau local 1 (carte réseau 1)

Le port réseau local 1 est un port réseau Ethernet RJ-45 10/100 Mbits/s à détection automatique et sert à connecter l'application à votre réseau existant. Pour plus d'informations sur les connexions, voir Etape 4 à la page 32.

Le port réseau local 1 reçoit et transmet le trafic suivant:

- Trafic du protocole entrant et sortant.
- Données de gestion et de journalisation, y compris les communications provenant du navigateur Web distant que vous utilisez pour accéder à l'interface utilisateur de l'application. Si vous utilisez le logiciel ePolicy Orchestrator (disponible séparément) avec l'application, ses communications sont également transmises via ce port.

L'adresse IP par défaut du port de données est 10.1.1.108 (masque de sous-réseau 255.255.255.0) qui vous permet d'accéder au départ à l'application par le réseau. Lorsque vous configurez l'application, vous pouvez:

- Ajouter une nouvelle adresse IP valide pour votre réseau.
- Modifier ou désactiver l'adresse IP par défaut.
- Supprimer l'adresse IP par défaut pour qu'elle ne soit plus utilisée.

REMARQUE : Dans les versions précédentes de l'application WebShield, le port réseau local 1 (LAN1) s'appelait *port de données*; la documentation existante peut comporter des références à cette notion.

Port réseau local 2 (carte réseau 2)

Le port réseau local 2 est un port réseau Ethernet RJ-45 10/100 Mbits/s à détection automatique et son fonctionnement dépend du mode d'utilisation de l'application:

- **Mode proxy** — Le port réseau local 2 peut uniquement être utilisé pour une connexion de gestion locale directe. Il *ne peut pas* recevoir ou transmettre de trafic de protocoles entrant et sortant.

  Vous pouvez utiliser ce port si vous ne parvenez pas à obtenir une connexion de gestion à distance via le port réseau local 1 à cause des raisons suivantes:

  – L'adresse IP du port réseau local 1 appartient à un sous-réseau différent de celui de votre ordinateur distant.

  – Vous avez oublié l'adresse IP du port réseau local 1 que vous avez définie et vous avez désactivé l'adresse IP par défaut (10.1.1.108) de ce port.

- **Mode transparence** — Le port réseau local 2 est utilisé (conjointement au port réseau local 1) pour connecter l'application au réseau existant. Il reçoit et transmet le même type de trafic que le port réseau local 1.

Pour plus d'informations sur les connexions, voir Etape 4 à la page 32.

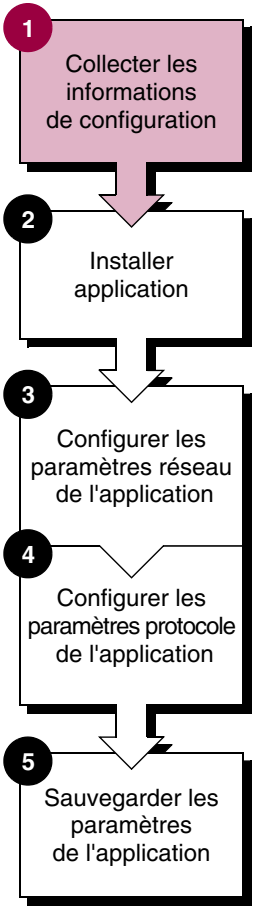
L'adresse IP par défaut du port réseau local 2 est 10.1.2.108 (masque de sous-réseau 255.255.255.0). Lorsque vous configurez l'application, vous pouvez:

- Ajouter une nouvelle adresse IP valide pour votre réseau.
- Modifier ou désactiver l'adresse IP par défaut.
- Supprimer l'adresse IP par défaut pour qu'elle ne soit plus utilisée.
- Désactiver le port pour qu'il ne soit plus utilisé.

IMPORTANT : Si vous utilisez le mode transparence, ne désactivez pas le port réseau local 2.

Dans les versions précédentes de l'application WebShield, le port réseau local 2 (LAN2) s'appelait *port de gestion*; la documentation existante peut comporter des références à cette notion.

Collecter les informations de configuration



Lorsque vous avez décidé de l'utilisation de l'application (voir chapitre 1 du Guide produit), vous êtes prêt à collecter les informations de configuration requises (étape 1).

Cette section répertorie les informations à fournir. Nous vous recommandons de collecter ces informations avant l'installation et la configuration, de façon à rapidement configurer l'application.

Nous avons laissé des espaces afin que vous puissiez enregistrer ces informations sur une version papier de la section.

Le chapitre 11 du Guide produit contient des informations utiles sur les informations de configuration que vous pouvez définir, ainsi que sur l'impact de la configuration sur le fonctionnement de l'application.

L'étape 2 — installation de l'application — est décrite page 31.

Nom d'hôte de l'application

Spécifiez un nom d'hôte unique pour l'application:

Nom d'hôte	

Domaine

Indiquez le domaine ou le sous-domaine entièrement qualifié où se trouve l'application:

Nom du domaine	

Exemples: `myorg.com`, `network1.myorg.com`

Adresses réseau

Indiquez l'adresse réseau TCP/IP de l'application:

	Adresse TCP/IP
adresse IP du port réseau local 1 et masque de sous-réseau	. . . . . .
adresse IP du port réseau local 2 et masque de sous-réseau	. . . . . .
Adresse IP du serveur DNS local	. . .
Adresse IP de la passerelle ou du routeur par défaut	. . .

❑ **REMARQUE :** Vous pouvez configurer plusieurs adresses IP pour les réseaux locaux 1 et 2.

Dans les précédentes versions de l'application WebShield, le port réseau local 1 s'appelait *port de données* et le port réseau local 2 s'appelait *port de gestion*. En conséquence, la documentation existante peut comporter des références à cette notion.

Réseaux internes

Indiquez les adresses IP ou les domaines des réseaux internes (à l'intérieur de votre entreprise) avec lesquels l'application communique. Vous pouvez identifier autant de réseaux internes que vous le souhaitez (l'espace ci-dessous est fourni pour 10 réseaux).

❑ **REMARQUE :** Pensez à inclure le domaine dans lequel est située l'application, à moins que vous vouliez que ce domaine soit considéré comme un réseau externe.

Réseau	Domaine, ou adresse IP et masque de sous-réseau
Exemple 1	myorg.com
Exemple 2	192 . 168 . 1 . 0 255 . 255 . 255 . 0
Exemple 3	*.myorg.com
1	

	. . . . . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . . . . .
7	. . . . . .
8	. . . . . .
9	. . . . . .
10	. . . . . .

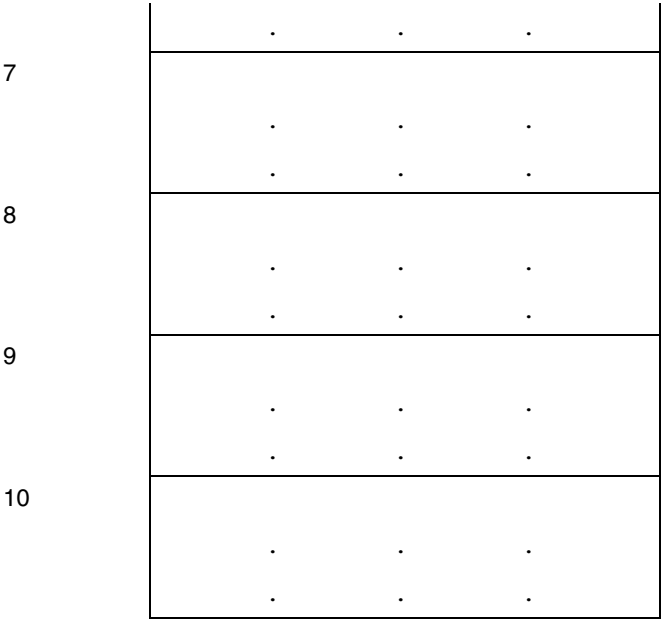
Réseaux externes

Indiquez les adresses IP ou les domaines des réseaux externes (à l'extérieur de votre entreprise) avec lesquels l'application communique. Vous pouvez identifier autant de réseaux externes que vous le souhaitez (l'espace ci-dessous est fourni pour 10 réseaux).

IMPORTANT : Nous vous recommandons de conserver l'entrée de domaine * dans vos réseaux externes, car elle garantit que l'application peut traiter le trafic Internet.

Veillez à préciser l'adresse IP du pare-feu.

Réseau	Domaine, ou adresse IP et masque de sous-réseau
Exemple 1	testing.myorg.com
Exemple 2	sales.myorg.com
Exemple 3	*
1	. . . . . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . .



Proxy ou transparence ?

Choisissez le mode utilisé par l'application (ce doit être l'un des modes suivants):

☐ Mode proxy (proxy explicite).

☐ Mode transparence (proxy transparent).

Pour plus d'informations sur ces modes, consultez la section « Proxy ou transparence ? » du Guide produit.

IMPORTANT : Comme les deux modes sont différents, il importe que vous sachiez lequel vous voulez utiliser *avant* d'installer l'application et de la configurer.

Chaque réseau étant différent, l'application doit être configurée avec les informations correctes pour que le réseau puisse fonctionner correctement. En cas de doute sur les informations à fournir, consultez l'administrateur réseau de votre entreprise.

Itinéraires statiques et routage dynamique

Lorsque vous intégrez l'application dans votre réseau, assurez-vous que toutes les parties du réseau peuvent continuer à communiquer aussi bien de façon interne qu'externe via l'application. Vous pouvez utiliser les itinéraires statiques et le routage dynamique pour configurer ces informations de telle sorte que l'application sache comment accéder aux différentes parties du réseau:

- **Mode proxy**: il existe certains cas dans lesquels l'application doit utiliser plusieurs passerelles ou routeurs pour communiquer avec tout le réseau. Définissez ces passerelles et routeurs additionnels comme itinéraires statiques.
- **Mode transparence**: il est parfois nécessaire de définir des informations de routage pour certaines communications internes et externes via l'application. Définissez ces informations de routage comme itinéraires statiques. En outre, comme l'application prend en charge les protocoles de routage RIP (Routing Information Protocol) et OSPF (Open Shortest Path First), vous pouvez utiliser le routage dynamique pour recueillir les informations de routage de votre réseau (sous réserve qu'il utilise ces protocoles).

Pour chaque itinéraire statique, indiquez l'adresse IP et le masque de sous-réseau pour identifier le réseau, et spécifiez l'adresse IP de la passerelle ou du routeur utilisé pour atteindre le réseau. Vous pouvez identifier autant d'itinéraires statiques que vous le souhaitez (l'espace ci-dessous est fourni pour 4 itinéraires).

Itinéraire	Adresse IP de réseau et masque de sous-réseau		Adresse IP de la passerelle ou du routeur
Exemple	192 . 168 . 40 . 0 255 . 255 . 255 . 0	→	192 . 168 . 50 . 3
1	. . . . . .	→	. . .
2	. . . . . .	→	. . .
3	. . . . . .	→	. . .
4	. . . . . .	→	. . .

Si vous souhaitez utiliser le routage dynamique pour obtenir les informations de routage, activez la case suivante:

☐ Activer le routage dynamique

Protocoles

Cochez les cases des serveurs proxy à activer et l'analyse des virus que vous souhaitez appliquer. Indiquez les ports sur lesquels votre réseau transfère le trafic des protocoles s'ils sont différents des ports par défaut (indiqués entre parenthèses):

	Activer le serveur proxy	Analyser le trafic entrant	Analyser le trafic sortant	Port
Messagerie électronique (SMTP)	☐	☐	☐	(25)
Transfert de fichiers (FTP)	☐	☐	☐	(21)
Navigation Web (HTTP)	☐	☐	☐	(80)
Téléchargement du courrier (POP3)	☐	☐		(110)

☐ **REMARQUE :** L'application analyse le trafic de téléchargement du courrier (POP3) sans distinction de direction (entrant ou sortant); voir "Téléchargement du courrier (POP3)" à la page 29. C'est pourquoi une seule case à cocher est disponible.

Profil d'analyse

Activez l'une des cases à cocher suivantes pour identifier le profil d'utilisation attendu:

- ☐ SMTP élevé constant, HTTP partiel, FTP minimum.
- ☐ SMTP modéré constant, HTTP constant, FTP minimum.
- ☐ SMTP très variable, HTTP constant, FTP minimum.
- ☐ Valeurs sélectionnées par l'utilisateur — L'application utilise les paramètres pertinents des pages de configuration des protocoles (interface utilisateur) pour vous permettre de spécifier les paramètres de configuration de votre choix.

☐ **REMARQUE :** Les profils d'utilisation ne mentionnent pas le protocole de téléchargement du courrier (POP3), car celui-ci est généralement utilisé moins souvent que les autres protocoles. Cependant, comme pour les autres serveurs proxy, les paramètres de configuration de chaque protocole peuvent être modifiés sur les pages de configuration du protocole (interface utilisateur), afin que des réglages supplémentaires puissent être effectués le cas échéant.

Les sections suivantes décrivent les informations complémentaires requises pour la configuration des différents protocoles: “Messagerie électronique (SMTP)” à la page 26, “Transfert de fichiers (FTP)” à la page 29 et “Téléchargement du courrier (POP3)” à la page 29.

Messagerie électronique (SMTP)

Activez les cases à cocher correspondant aux méthodes de remise requises:

- ☐ Domaines configurés en local; voir ci-dessous.
- ☐ DNS.

  L'application utilise le serveur DNS spécifié lorsque vous avez fourni les informations d'adresse de réseau TCP/IP; voir “Adresses réseau” à la page 20.

- ☐ Relais de repli; voir page 28.

Domaines configurés localement

Fournissez les informations suivantes pour les relais de messagerie: Vous pouvez créer autant de relais que vous le souhaitez (un espace est fourni ci-dessous pour 15 relais). Identifiez en premier les relais les plus courants, car l'application essaie les relais dans l'ordre où ils sont indiqués.

Relais	Domaine de messagerie électronique		Hôtes qualifiés complets (serveurs de messagerie)
Exemple 1	*myorg.com*	→	*mail.uk.myorg.com*
Exemple 2	*myorg.co.uk*	→	*mail1.us.myorg.com mail2.us.myorg.com*
Exemple 3	**.myorg2.com*	→	*mail2.us.myorg.com*
1		→	
2		→	
3		→	
4		→	
5		→	
6		→	
7		→	
8		→	
9		→	
10		→	
11		→	
12		→	
13		→	
14		→	
15		→	

Relais de repli

Fournissez les informations suivantes pour les relais de repli: Vous pouvez créer autant de relais que vous le souhaitez (un espace est fourni ci-dessous pour 15 relais). Identifiez en premier les relais les plus courants, car l'application essaie les relais dans l'ordre où ils sont indiqués.

Relais	Domaine de messagerie électronique		Hôtes qualifiés complets
Exemple 1	*myorg.org*	→	*mail.externalorg1.com mail.externalorg2.com*
Exemple 2	*	→	*outmail.myorg.com*
1		→	
2		→	
3		→	
4		→	
5		→	
6		→	
7		→	
8		→	
9		→	
10		→	
11		→	
12		→	
13		→	
14		→	
15		→	

Transfert de fichiers (FTP)

Pour bloquer les transferts ASCII 8 bits, activez la case à cocher suivante:

☐ Bloquer le transfert de données 8 bits en mode ASCII.

❑ **REMARQUE :** Certains utilitaires de transfert de fichiers utilisant par défaut le mode ASCII 8 bits, vous devez penser à configurer vos utilitaires en mode binaire si l'application bloque le transfert des données en mode ASCII à 8 bits.

Pour plus d'informations sur le transfert FTP, reportez-vous au Guide produit.

Téléchargement du courrier (POP3)

Proxy générique

Lorsqu'une connexion proxy générique est effectuée via l'application, celle-ci sépare le nom d'utilisateur, le nom d'hôte et le numéro de port à l'aide des caractères de séparation dièse (#) et deux-points (:):

```
utilisateur#hôte:port
```

Pour utiliser d'autres caractères de séparation, indiquez-les ici:

utilisateur ☐ hôte ☐ port

❑ **REMARQUE :** Lorsque vous configurez l'application avec un numéro de port pour des connexions génériques, vos clients POP3 (logiciel) n'ont pas besoin de spécifier ce numéro de port chaque fois qu'ils établissent une connexion POP3 générique via l'application.

Proxy dédié

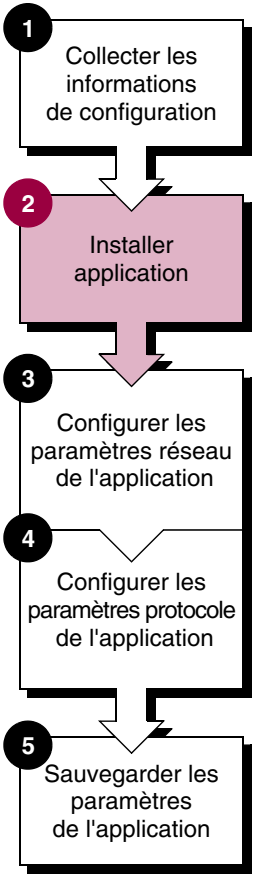
Lorsqu'un utilisateur établit une connexion proxy dédiée via l'application, cette dernière utilise un port spécifique pour contacter le serveur POP3.

Vous pouvez autoriser des connexions vers autant de serveurs que vous le souhaitez (un espace est fourni ci-dessous pour 10 serveurs). Indiquez le numéro de port et le nom de domaine de chaque serveur:

Serveur	Port	Nom de domaine du serveur POP3
Exemple	*1024*	*pop3server.externalorg.com*
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Pour plus d'informations sur POP3, reportez-vous au Guide produit.

Installation de l'application



Une fois que vous avez rassemblé les informations de configuration requises (voir page 19), vous êtes prêt à installer l'application dans l'emplacement souhaité et à établir les connexions requises (étape 2).

Le présent chapitre décrit la procédure d'installation. Nous vous recommandons de lire au préalable cette procédure, afin d'être certain de connaître les éléments requis.

Pour la liste des éléments complémentaires requis, voir page 11.

L'étape 3 — configuration des paramètres réseau de l'application — est décrite page 35.

Pour plus d'informations sur les ports et connecteurs de l'application, voir page 14.

Pour installer l'application WebShield e500:

1. Lisez les avertissements de sécurité de “Informations sur l'alimentation et la sécurité” à la page 3 et veillez à toujours les respecter.
2. Retirez l'application WebShield e500 de son emballage protecteur et placez-la sur une surface plane.
3. Si vous prévoyez d'installer l'application à un emplacement particulier, comme un rack 19 pouces, effectuez la procédure suivante en veillant à respecter les avertissements de sécurité; voir “Informations sur l'alimentation et la sécurité” à la page 3:

   a. Préparez l'emplacement prévu.

      Vous pouvez utiliser le kit de montage pour installer l'application WebShield e500 dans un rack 19 pouces. Suivez les instructions page viii (en début du présent guide).

      Prévoyez un passage suffisant pour l'aération et l'accès aux ports et connecteurs de l'application.

b. Installez l'application à l'emplacement prévu.

Vérifiez que l'application est fermement maintenue en place et ne risque pas de tomber.

4. À l'aide des câbles réseau fournis, connectez l'application au réseau. Les ports et câbles utilisés dépendent du mode d'utilisation de l'application:

- **Mode Proxy**

Port réseau local 1:A l'aide du câble réseau bleu fourni — ou d'un câble réseau Ethernet de catégorie 5 équivalent — connectez le port réseau local 1 de l'application (voir H page 17) au réseau existant (Figure 3-2). Il s'agit d'un câble droit (non croisé), vous permettant de connecter l'application à un port RJ-45 non croisé standard (MDI) de votre équipement réseau.

Cette connexion permet aussi de gérer l'application depuis un ordinateur distant à travers le réseau.

Port réseau local 2: En mode proxy, le port réseau local 2 de l'application devient un port de gestion dédié. Si vous prévoyez de gérer l'application en local, utilisez le câble réseau de couleur orange fourni — ou un câble Ethernet croisé équivalent de catégorie 5 — pour connecter le port réseau local 2 (voir I page 18) à la carte réseau de l'ordinateur local (Figure 3-2).

Cette connexion n'est nécessaire que si vous prévoyez de gérer l'application localement.

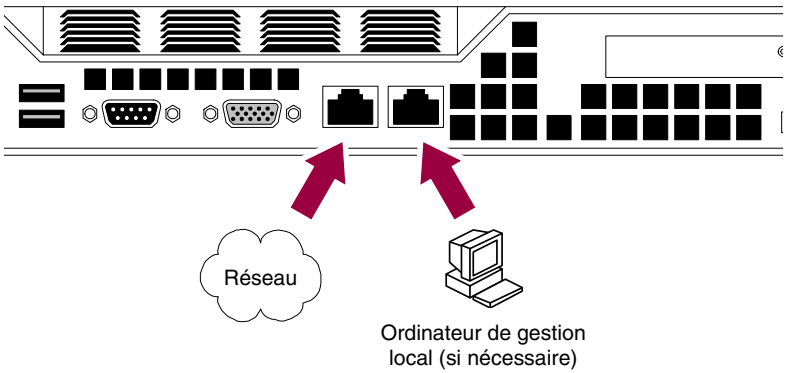


Figure 3-2. Connexion de votre application (mode proxy)

- **Mode Transparence**

  Ports réseau local 1 et réseau local 2:A l'aide des câbles réseau de couleur bleue — ou de câbles Ethernet de catégorie 5 équivalents — connectez le port réseau local 1 de l'application (voir H page 17) et le port réseau local 2 (voir I page 18) à votre réseau existant (Figure 3-3) afin d'insérer l'application dans le flux de données. Comme il s'agit de câbles droits (non croisés), vous pouvez connecter l'application aux port RJ-45 non croisés standard (MDI) de votre équipement réseau.

  ☐ **REMARQUE :** En mode transparence, l'application doit être connectée à deux sous-réseaux différents.

  L'application doit être utilisée *à l'intérieur du* pare-feu. Par exemple, si votre réseau est connecté à Internet via un concentrateur et un pare-feu, vous pouvez placer l'application entre le concentrateur et le pare-feu (en connectant le concentrateur au port réseau local 1 et le pare-feu au port réseau local 2).

  Cette connexion permet aussi de gérer l'application depuis un ordinateur distant à travers le réseau. Cependant, vous ne pouvez pas obtenir une connexion de gestion locale via le port réseau local 2 (méthode disponible avec le mode proxy) car ce port est obligatoire pour la réception et la transmission du trafic.

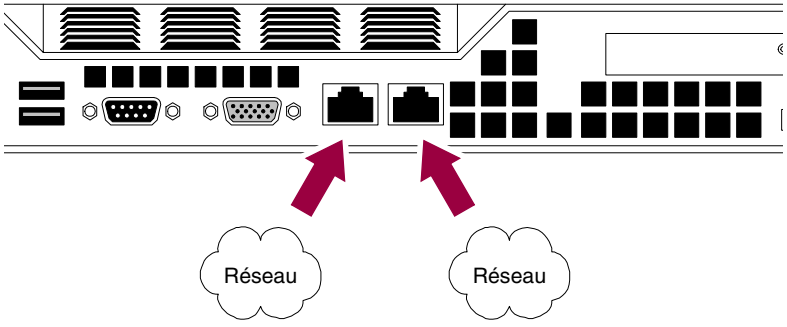


Figure 3-3. Connexion de votre application (mode transparence)

5. Utilisez le cordon d'alimentation fourni pour raccorder l'application (voir D page 16) à une prise électrique en état de fonctionnement.

IMPORTANT : Vérifiez la compatibilité du cordon d'alimentation dans le pays d'utilisation. S'il ne convient pas, contactez votre fournisseur.

Le logiciel de l'application étant préinstallé, n'insérez pas de CD-ROM dans le lecteur de CD-ROM sauf recommandation expresse contraire.

---

6. Mettez l'application sous tension en faisant basculer le bouton de mise sous tension et le bouton de marche/arrêt en position de marche (Figure 3-4).

   Le bouton de mise sous tension se trouve à l'arrière de l'unité (voir E page 16). Le bouton de marche/arrêt se trouve sur le panneau de contrôle, à l'avant de l'unité (voir C page 15).

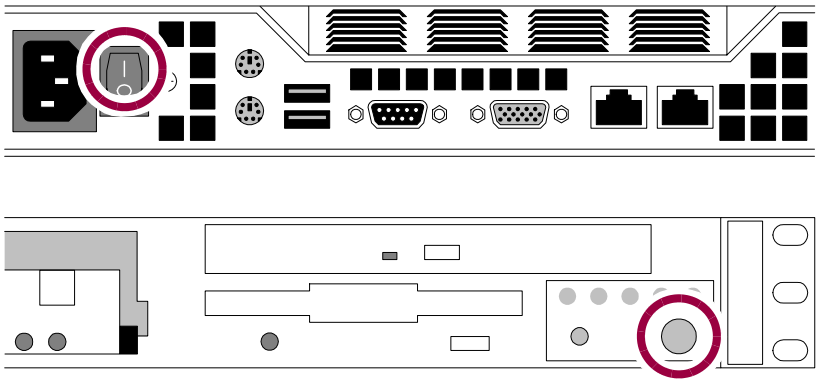


Figure 3-4. Mise en marche de l'application

L'application exécute sa séquence d'amorçage et est opérationnelle après environ deux minutes. Vous pouvez à présent configurer les paramètres de protocole de l'application; passez à la section page 35.

Configuration des paramètres réseau

Une fois l'application installée à l'emplacement de votre choix et les connexions nécessaires effectuées (voir page 31), vous êtes prêt à configurer les paramètres réseau de l'application (étape 3).

La présente section décrit la procédure de configuration des paramètres réseau. Nous vous recommandons de lire au préalable cette procédure, afin d'être certain de connaître les éléments requis.

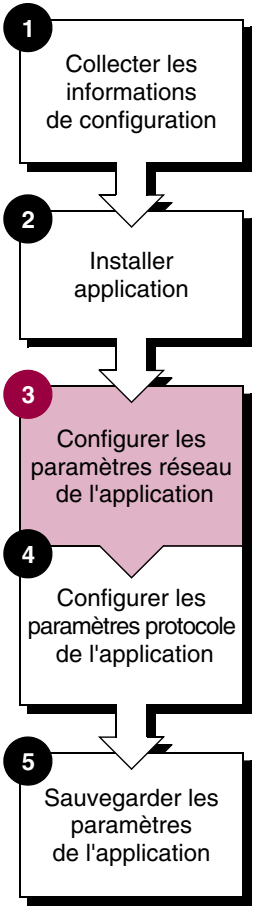
Si vous avez déjà réuni les informations de configuration nécessaires (voir page 19), vous pourrez configurer plus rapidement l'application.

Pour restaurer ou mettre à niveau le logiciel de l'application, voir page 63.

Si vous avez précédemment créé un ensemble de fichiers de configuration à partir desquels vous voulez restaurer les paramètres de l'application, voir "Restauration de vos paramètres" à la page 62.

L'étape 4 — configuration des paramètres protocole de l'application — est décrite page 45.

Pour plus d'informations sur les paramètres par défaut de l'application, reportez-vous à l'annexe A du Guide produit.



Pour configurer les paramètres réseau de l'application:

1. Ouvrez le navigateur Web depuis l'ordinateur que vous souhaitez utiliser pour gérer l'application.
2. Dans le champ adresse — où vous pouvez taper une URL (Uniform Resource Locator) pour ouvrir un site Web — saisissez l'adresse suivante:

   `https://<adresse IP>`

   REMARQUE : Veillez à taper `https`, et non `http`.

   L'`<adresse IP>` que vous utilisez dépend de votre connexion à l'application:

   - Accès à distance (à travers le réseau), via le port réseau local 1 — Utilisez l'adresse IP du port réseau local 1 configurée pour l'application (c' est `10.1.1.108` par défaut).
   - Accès à distance (à travers le réseau), via le port local LAN2 — Utilisez l'adresse IP du port réseau local 2 configurée pour l'application (`10.1.1.108` par défaut).

- Accès local, directement connecté au port réseau local LAN2 (disponible en mode proxy uniquement) — Utilisez l'adresse IP du port réseau local 2 configurée pour l'application (c' est `10.1.1.108` par défaut).

☐ **REMARQUE :** Si vous utilisez l'application en mode transparence, utilisez l'adresse IP du port et du sous-réseau auxquels votre ordinateur de gestion est connecté.

Toutes les connexions de gestion utilisent le cryptage SSL (Secure Sockets Layer), elles sont donc sécurisées. La connexion SSL se ferme lorsque vous terminez la session de gestion en cliquant sur **Fermer la session**. Afin de garantir la sécurité dans le cas de sessions de gestion longues, la connexion SSL se ferme automatiquement au bout de 15 minutes d'inactivité.

Lors de la configuration de nouvelles adresses IP des ports réseau local 1 et 2 (Etape 16 à la page 40), l'application *ajoute* la nouvelle adresse aux ports; elle ne remplace pas les adresses IP par défaut. Si vous utilisez l'application en mode proxy, l'adresse IP du port réseau local 2 est une adresse distincte, réservée à ce seul port (elle ne peut pas être vue par le port réseau local 1) et vous ne pouvez pas la désactiver.
Vous pouvez utiliser le port réseau local 2 pour un accès de gestion direct si vous ne parvenez pas à accéder au port réseau local 1.

Vous devez vous assurer l'application n'est pas configurée en tant que serveur proxy du navigateur Web qui se trouve sur l'ordinateur de gestion (ordinateur utilisé pour gérer l'application). Si c'est le cas, la connexion de gestion ne fonctionnera pas.

En outre, si un serveur proxy se trouve entre l'ordinateur de gestion et l'application, il doit être configuré en tant qu'hôte de remise de l'application.

---

3. Lorsque le navigateur Web trouve l'application, il se peut qu'une alerte de sécurité s'affiche, vous demandant d'accepter le certificat de sécurité de l'application. Cliquez sur **Oui** pour accepter le certificat.

   ASTUCE : L'alerte de sécurité peut s'afficher à chaque démarrage d'une session du navigateur. Pour empêcher cela, vous pouvez afficher et installer le certificat de façon à ce qu'il soit automatiquement accepté. Pour ce faire, sous Internet Explorer, cliquez sur **Afficher le certificat** dans la boîte de dialogue Alerte de sécurité, puis sur **Installer le certificat** dans la boîte de dialogue qui s'affiche.

   Si vous venez d'allumer l'application, vous devez patienter environ deux minutes pour que la séquence d'amorçage s'exécute, ou bien le navigateur Web risque de ne pas trouver l'application à la première tentative. Si tel est le cas, entrez à nouveau l'URL. Si vous ne parvenez toujours pas à accéder à la page « Connexion », voir page 70.

   La page « Connexion » de l'application s'affiche. L'application contrôle le navigateur Web afin de s'assurer qu'il est pris en charge et qu'il contient le code requis pour exécuter l'interface de l'application. C'est pourquoi plusieurs alertes de sécurité et boîtes de dialogue de téléchargement peuvent s'afficher. Complétez ces boîtes de dialogues selon les besoins.

   REMARQUE : L'interface utilisateur de l'application nécessite le logiciel Java 2 Runtime Environment. Si votre navigateur Web requiert son installation, vous devez savoir que la taille du logiciel est de 5 à 14 Mo (selon les composants requis par votre navigateur) et que l'installation peut prendre du temps si votre liaison distante à l'application est peu rapide.

4. Dans **Langue**, sélectionnez la langue dans laquelle l'interface de l'application doit être affichée.

   Cette sélection n'a aucune influence sur le langage dans lequel l'application s'exécute; voir Etape 14 à la page 40.

5. Si vous choisissez Anglais comme langue, sélectionnez Local. Vous pouvez ainsi utiliser un autre jeu de caractères que le jeu anglais lors de l'utilisation de l'interface.

6. Cliquez sur **Ouvrir la session**.

   La boîte de dialogue de saisie du mot de passe réseau s'affiche, vous demandant vos nom et mot de passe utilisateur. Le nom d'utilisateur est `e500` et le mot de passe par défaut `e500changeme`. Si vous avez récemment restauré le logiciel de l'application sans conserver les paramètres précédents, le mot de passe est de nouveau le mot de passe par défaut.

7. Tapez les nom et mot de passe utilisateur, puis cliquez sur **OK**.

   L'interface utilisateur de l'application s'affiche à la page Configuration du système.

   Si vous avez déjà configuré l'application auparavant, c'est la page Etat du système qui apparaît avec une barre de navigation sur la gauche. Pour afficher la page Configuration du système, sélectionnez **Configuration du système** dans la barre de navigation. Pour plus d'informations sur l'interface utilisateur, voir "Utilisation de l'application" à la page 59. Pour plus d'informations sur la configuration d'une page particulière, affichez la rubrique d'aide correspondante en cliquant sur le bouton d'aide de cette page.

   ❑ **REMARQUE :** Si vous possédez un fichier de configuration provenant d'une version antérieure de l'application, utilisez le panneau Restaurer la configuration pour rétablir ces paramètres; voir "Restauration de vos paramètres" à la page 62.

   ---

8. Dans la zone de texte **Nom de l'hôte**, tapez un nom d'hôte pour l'application; ce nom ne doit pas dépasser 15 caractères (voir "Nom d'hôte de l'application" à la page 19).

9. Dans la zone de texte **Serveur DNS**, tapez l'adresse IP du serveur DNS local.

10. Dans la zone de texte **Nom du domaine**, tapez le nom du domaine ou du sous-domaine sur lequel se trouve l'application, par exemple `myorg.com` (voir "Domaine" à la page 19).

11. Dans la zone de texte **Serveur DNS**, tapez l'adresse IP du serveur DNS local (voir "Adresses réseau" à la page 20).

12. Si l'application communique avec le réseau via une passerelle ou un routeur (firewall) par défaut, tapez l'adresse IP de la passerelle ou du routeur dans la zone de texte **Passerelle par défaut** (voir “Adresses réseau” à la page 20).

    Si vous utilisez l’application en mode Proxy, il existe certains cas dans lesquels l’application doit utiliser plusieurs passerelles ou routeurs pour communiquer avec tout le réseau. En cas de nécessité, vous pouvez définir ces routeurs et passerelles supplémentaires comme itinéraires statiques; voir Etape 22 à la page 43.

13. Pour utiliser l'application en mode transparence, sélectionnez **Activer la transparence**. Sinon, n'activez pas la case à cocher pour utiliser l'application en mode proxy (voir “Proxy ou transparence ?” à la page 23).

14. Dans **Langue système**, sélectionnez la langue dans laquelle vous voulez que l’application fonctionne.

    Ce paramètre affecte les rapports et les messages générés par l’application, à l’exception des chaînes de texte que vous pouvez spécifier ou modifier via l’interface. Il s’agit par ailleurs d’un paramètre différent de la langue utilisée pour l’affichage de l'interface (choisie quand vous vous connectez à l’application); voir Etape 4 à la page 38).

15. Si le panneau Adresses IP du LAN n'apparaît pas, cliquez sur **Adresses IP du LAN** pour afficher le panneau.

    Ce panneau répertorie les adresses IP configurées pour les ports LAN1 et LAN2.

16. Utilisez les boutons **Ajouter** sous les listes LAN1 et LAN2 pour spécifier les nouvelles adresses IP de ces ports (voir “Adresses réseau” à la page 20).

    Vous pouvez définir plusieurs adresses IP pour chaque port. L'application les ajoute aux ports quand vous appliquez les modifications (Etape 27 à la page 44). Les nouvelles adresses IP n'écrasent pas les adresses IP existantes. Si vous ne voulez plus utiliser une adresse IP, vous pouvez:

    - Modifier ou désactiver l'adresse IP — sélectionnez-la dans la liste et cliquez sur **Modifier**. Pour la désactiver, sélectionnez **Désactiver l'adresse réseau**.

- Supprimer l'adresse IP — sélectionnez-la dans la liste et cliquez sur **Supprimer**.

> **REMARQUE :** Nous vous recommandons d'accéder à l'application à l'aide des nouvelles adresses IP (après la configuration initiale) *avant* de supprimer les adresses IP par défaut, pour être certain que les nouvelles adresses fonctionnent.

Si vous utilisez l'application en mode proxy, le port LAN2 devient un port de gestion dédié et vous pouvez établir une connexion directe de gestion locale.

17. Pour empêcher les connexions de gestion directes à l'application, désactivez le port LAN2. Pour cela, sélectionnez **Désactiver** sous la liste LAN2.

> **IMPORTANT :** Si vous utilisez le mode transparence, ne désactivez pas le port réseau local 2.

L'application utilise deux listes (Réseaux intérieurs et Réseaux extérieurs) pour déterminer si la source du trafic qui la traverse est interne ou externe.

> **ASTUCE :** Si vous avez spécifié des sous-domaines internes que vous voulez voir traités comme des réseaux externes, par exemple `testing.myorg.com`, vous pouvez utiliser les listes Réseaux intérieurs et Réseaux extérieurs comme suit:
>
> Réseaux intérieurs:
>
> ```
> *.myorg.com
> ```
>
> Réseaux extérieurs:
>
> ```
> testing.myorg.com
>
> *
> ```

18. Cliquez sur **Réseaux intérieurs** pour afficher le panneau Réseaux intérieurs.

19. Utilisez ce panneau pour définir les domaines ou sous-réseaux IP des réseaux internes au sein de votre entreprise (à l'intérieur du pare-feu) que vous voulez protéger à l'aide de l'application (voir "Réseaux internes" à la page 20). Vous pouvez spécifier autant de réseaux que vous le souhaitez.

❒ **REMARQUE :** Si vous souhaitez que l'application protège le domaine sur lequel se trouve l'application (spécifié à l'Etape 10 à la page 39), vous devez ajouter ce domaine à la liste Réseaux intérieurs.

Pour ajouter un réseau, cliquez sur **Ajouter**, puis indiquez le domaine ou l'adresse IP et le masque de sous-réseau dans la boîte de dialogue d'ajout qui s'affiche. Cliquez sur **OK** pour l'ajouter à la liste Réseaux intérieurs.

20. Cliquez sur **Réseaux externes** pour afficher le panneau Réseaux externes.

    Ce panneau affiche les réseaux configurés comme externes à l'application. Par défaut, l'application utilise le caractère générique astérisque (*) dans la liste Réseaux extérieurs pour indiquer que tous les réseaux (autres que ceux définis dans la liste Réseaux intérieurs) sont des réseaux extérieurs.

IMPORTANT : Nous vous recommandons de conserver l'entrée de domaine `*` dans vos réseaux externes, car elle garantit que l'application peut traiter le trafic Internet.

Veillez à préciser l'adresse IP du pare-feu.

---

21. Utilisez ce panneau pour spécifier les domaines ou sous-réseaux IP des réseaux externes à l'extérieur de votre entreprise (à l'extérieur du pare-feu). Vous pouvez spécifier autant de réseaux que vous voulez (voir “Réseaux externes” à la page 22).

    Pour ajouter un réseau, cliquez sur **Ajouter**, puis indiquez le domaine ou l'adresse IP et le masque de sous-réseau dans la boîte de dialogue d'ajout qui s'affiche. Cliquez sur **OK** pour l'ajouter à la liste Réseaux extérieurs.

22. Si vous devez définir certains itinéraires statiques pour différentes parties du réseau de façon à ce que l'application sache comment les atteindre (voir “Itinéraires statiques et routage dynamique” à la page 24), cliquez sur **Itinéraires statiques** et définissez ces itinéraires dans le panneau Itinéraires statiques.

23. Si vous utilisez l'application en mode transparence et souhaitez utiliser le routage dynamique, cliquez sur **Itinéraires dynamiques**, puis sélectionnez **Activer le routage dynamique**.

    Le routage dynamique est un système qui permet à votre dispositif de réseau (y compris à l'application) d’être à l’écoute des informations de routage diffusées par les routeurs de votre réseau. Rappelez-vous que l'application prend en charge uniquement les protocoles de routage RIP (Routing Information Protocol) et OSPF (Open Shortest Path First).

24. Cliquez sur **Time and Password Settings (Paramètres d'heure et de mot de passe)** pour afficher le panneau Time and Password Settings (Paramètres d'heure et de mot de passe).

25. Modifiez les valeurs des champs **Fuseau horaire**, **Date** et **Heure** pour qu'elles correspondent aux date et heure actuelles, puis cliquez sur **Définir maintenant**. L'heure est au format 24 heures.

    L'application modifie ses valeurs de date et d'heure. Ces valeurs sont utilisées pour l'horodatage du trafic passant par l'application, ainsi que pour la journalisation et les alertes.

26. Pour modifier le mot de passe, tapez le nouveau mot de passe dans la zone de texte **Mot de passe**, puis tapez-le à nouveau dans la zone de texte **Confirmer**. Cliquez sur **Définir maintenant**.

    IMPORTANT : Pour des raisons de sécurité, il est fortement recommandé de modifier maintenant le mot de passe par défaut (lorsque vous configurez l'application pour la première fois).

27. Cliquez sur **Appliquer toutes les modifications**.

    Le navigateur Web envoie vos modifications à l'application. L'interface utilisateur vous demande de redémarrer le logiciel de l'application car vous avez modifié la configuration IP.

28. Cliquez sur **Redémarrer maintenant**.

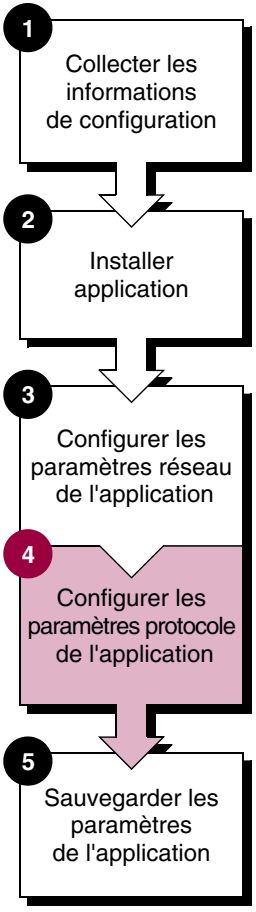
    L'application redémarre son logiciel et est opérationnelle après environ deux minutes.

    L'interface utilisateur affiche un nouveau lien hypertexte de l'URL que vous pouvez utiliser pour accéder de nouveau à l'interface utilisateur avec la nouvelle adresse IP.

29. Lorsque l'application a redémarré, cliquez sur le lien hypertexte ou utilisez l'une des autres adresses IP que vous avez configurées pour le port que vous utilisez pour gérer l'application. Si vous utilisiez le port LAN2 mais que vous décidez de désactiver son adresse IP (Etape 17 à la page 41), accédez au port LAN1 par le réseau.

    Une fois que vous êtes connecté, la page Etat du système apparaît avec une barre de navigation sur la gauche. Vous pouvez à présent configurer les paramètres de protocole de l'application; passez à la section “Configuration des paramètres de protocole” à la page 45.

Configuration des paramètres de protocole



Lorsque vous avez configuré les paramètres réseau de l'application (voir page 35), vous êtes prêt à configurer les paramètres de protocole de l'application (étape 4).

La présente section décrit la procédure de configuration des paramètres de protocole. Nous vous recommandons de lire au préalable cette procédure, afin d'être certain de connaître les éléments requis.

Si vous avez déjà réuni les informations de configuration nécessaires (voir page 19), vous pourrez configurer plus rapidement l'application.

L'étape 5 — sauvegarde des paramètres de l'application — est décrite page 61.

Tâches

Cette section est découpée en fonction des tâches suivantes que vous devez effectuer dans l'ordre:

1. Configuration des protocoles de l'application; voir page 46.
2. Configuration de la fonctionnalité de mise à jour automatique, afin de maintenir à jour le fichier de définition des virus (.DAT) et le moteur d'analyse de l'application et d'assurer une protection antivirus totale; voir page 52.
3. Si nécessaire, configurez le pare-feu, le serveur de messagerie, le cache Web et d'autres équipements pour acheminer le trafic via l'application; voir page 53.
4. Test de votre configuration, afin de s'assurer que les trafics entrant et sortant sont correctement analysés pour la recherche de virus; voir page 55.

Configuration des protocoles de l'application

L'application WebShield e500 fournit des serveurs proxy pour les protocoles SMTP, FTP, HTTP et POP3. Par défaut, elle répartit ses ressources entre les différents serveurs proxy, analysant les virus pour chaque trafic entrant et sortant du protocole (pas de distinction du sens du trafic POP3). Pour plus d'informations sur les serveurs proxy et les protocoles, voir "Ports et connecteurs" à la page 14.

Pour définir quels protocoles activer et quels virus rechercher, et pour sélectionner le profil utilisateur approprié:

1. Pour désactiver les serveurs proxy pour un protocole — pour empêcher le trafic du protocole de traverser l'application — décochez les cases appropriées dans la section **Protocoles activés** de la page Configuration du système.

   ☐ **REMARQUE :** En mode transparence, le passage du trafic est toujours acheminé à travers l'application.

2. Pour désactiver l'analyse de virus du trafic entrant ou sortant pour l'un des protocoles activés, sélectionnez la page **Configuration** appropriée dans la barre de navigation (Configuration de la messagerie électronique, Configuration de transfert de fichiers, Configuration de la navigation Web ou Configuration de téléchargement de courrier), puis désélectionnez **Analyser le trafic entrant** ou **Analyser le trafic sortant** selon vos besoins (**Analyser le trafic POP3** est utilisé sur la page Configuration du téléchargement du courrier).

   AVERTISSEMENT : Ne désactivez pas l'analyse des virus pour un protocole activé *sauf* si vous analysez son trafic à un autre point du réseau. Autoriser un trafic non analysé à entrer et quitter votre organisation vous laisse sans défense contre une infection éventuelle par des virus.

   Vérifiez que vous avez configuré le reste de votre équipement réseau pour acheminer les protocoles via l'application, afin que rien ne puisse contourner l'application; voir page 53.

3. Dans la barre de navigation, sélectionnez **Profils système**.

4. Sélectionnez le profil d'utilisation le plus approprié (voir “Profil d'analyse” à la page 26).

   Les profils d'utilisation ne mentionnent pas le protocole de téléchargement du courrier (POP3), car celui-ci utilise une plus petite bande passante que les autres protocoles. Si vous avez activé l'analyse pour le protocole POP3, il est analysé quel que soit le profil que vous sélectionnez.

   Vous pouvez régler toutes les autres valeurs d'usage (y compris les niveaux du POP3) dans les pages Configuration des différents protocoles. Si vous le faites, l'application sélectionne automatiquement **Valeurs sélectionnées par l'utilisateur dans « Configuration » pour chaque protocole** dans la page Profils système.

5. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Configuration des ports utilisés pour les protocoles

L'application utilise les ports par défaut suivants pour les protocoles:

- Messagerie électronique (SMTP): 25
- Transfert de fichiers (FTP): 21
- Navigation Web (HTTP): 80
- Téléchargement du courrier (POP3): 110

Si le réseau de votre entreprise utilise des ports différents pour les protocoles, vous devez modifier les numéros des ports de l'application en conséquence.

Pour changer le port utilisé pour un protocole:

1. Dans la barre de navigation, sélectionnez la page **Configuration** du protocole.
2. Dans la zone de texte **Port d'écoute...**, tapez le numéro de port requis (voir “Protocoles” à la page 25).
3. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Configuration des méthodes de remise du courrier (SMTP)

Si un protocole de messagerie est activé (paramètre par défaut), vous devez configurer les méthodes de remise de courrier qu'il utilise.

Cette section fournit uniquement les informations nécessaires à la configuration des méthodes de remise du courrier pour que l'application puisse commencer à analyser et transmettre le trafic. Il existe de nombreuses pages de fonctionnalités associées à ce protocole; pour plus d'informations sur la configuration de ces pages, consultez les rubriques d'aide correspondantes en cliquant sur le bouton d'aide ; voir page 59.

Pour configurer les méthodes de remise du courrier électronique:

1. Dans la barre de navigation, sélectionnez **Remise du courrier électronique**.
2. Dans le panneau Méthodes utilisées, sélectionnez les méthodes de remise du courrier requises (voir "Messagerie électronique (SMTP)" à la page 26).
3. Si vous avez sélectionné la méthode de remise de courrier **Domaines locaux**, cliquez sur **Domaines locaux** et spécifiez les relais de messagerie dans le panneau qui s'affiche. Vous pouvez spécifier autant de relais de messagerie que vous le souhaitez (voir "Domaines configurés localement" à la page 27).

   Les relais de messagerie acheminent les messages électroniques destinés à des domaines spécifiques (tels que myorg.com) jusqu'aux serveurs de messageries appropriés (tels que mail1.myorg.com). Pour ajouter un relai de messagerie, cliquez sur **Ajouter**, puis spécifiez le domaine et l'hôte (serveur de messagerie) de courrier électronique dans la boîte de dialogue d'ajout qui s'affiche. Cliquez sur **OK** pour l'ajouter à la liste Domaines locaux.

> **ASTUCE :** L'application teste les relais de messagerie dans l'ordre. Si l'un de ces relais est permet à un message d'aboutir, les autres relais ne sont pas testés pour ce message. Aussi, utilisez les boutons **Déplacer vers le haut** et **Déplacer vers le bas** pour positionner les relais dans l'ordre de votre choix. Placez les relais qui sont le plus fréquemment utilisés en haut de la liste.

4. Si vous avez sélectionné la méthode de remise de courrier **Relais de repli**, cliquez sur **Relais de repli** et spécifiez les relais de repli dans le panneau qui s'affiche. Vous pouvez spécifier autant de relais de repli que vous le souhaitez (voir "Relais de repli" à la page 28).

   Les relais de repli acheminent les messages électroniques qui ne peuvent pas être délivrés à l'aide des autres méthodes de remise de courrier. Pour ajouter un relai de repli, cliquez sur **Ajouter**, puis spécifiez le domaine ou l'hôte (serveur de messagerie) de messagerie électronique dans la boîte de dialogue d'ajout qui s'affiche. Cliquez sur **OK** pour l'ajouter à la liste Relais de repli.

   ASTUCE : Vous pouvez créer un relais de repli pour acheminer des messages depuis tous les domaines en utilisant le caractère générique astérisque (*) pour le domaine. Si l'entrée du caractère générique est placée sous d'autres entrées de la liste Relais de repli (comme indiqué à la), l'application essaiera les autres entrées avant celle du caractère générique.

   La liste des relais de repli peut contenir des relais pour les hôtes locaux (serveurs de messagerie). De cette façon, vous avez la possibilité d'essayer des domaines locaux *après* une recherche du serveur DNS, afin d'acheminer des messages non remis dans l'entreprise.

   L'application teste les relais de messagerie dans l'ordre. Si l'un de ces relais est permet à un message d'aboutir, les autres relais ne sont pas testés pour ce message. Aussi, utilisez les boutons **Déplacer vers le haut** et **Déplacer vers le bas** pour positionner les relais dans l'ordre de votre choix. Placez les relais qui sont le plus fréquemment utilisés en haut de la liste.

   ---

5. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Configuration de l'autorisation des transferts de données 8 bits

Le protocole de transfert de fichiers (FTP) autorise deux modes de transfert de données entre ordinateurs: le mode binaire et le mode ASCII (American Standard Code for Information Interchange) 8 bits. Le mode binaire est cohérent à travers les plates-formes d'ordinateurs, permettant ainsi une analyse efficace des données.

REMARQUE : Par défaut, l'application bloque le mode de transfert à 8 bits en mode ASCII, car ses données contiennent différents codes et mises en forme de caractères (selon le système informatique utilisé), ce qui permet aux virus de facilement se dissimuler.

Si le protocole de transfert de fichiers est activé (paramètre par défaut), vous pouvez activer les transferts de données 8 bits.

Pour activer les transferts de données 8 bits:

1. Dans la barre de navigation, sélectionnez **Configuration de transfert de fichiers**.
2. Désélectionnez **Bloquer le transfert de données à 8 bits en mode ASCII** (voir "Transfert de fichiers (FTP)" à la page 29).
3. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

   REMARQUE : Certains utilitaires de transfert de fichiers utilisent le mode ASCII à 8 bits par défaut, aussi devez-vous penser à modifier vos utilitaires pour qu'ils passent en mode binaire.

Configuration des serveurs proxy de téléchargement du courrier (POP3)

Si le protocole de téléchargement du courrier est activé (paramètre par défaut), vous pouvez configurer les caractères de séparation (pour les connexions proxy génériques) et les numéros de port (pour les connexions proxy dédiées).

Par défaut, lorsqu'un utilisateur effectue une connexion proxy générique via l'application, celle-ci sépare le nom d'utilisateur, le nom d'hôte et le numéro de port à l'aide des caractères de séparation dièse (#) et deux-points (:):

```
utilisateur#hôte:port
```

Pour changer les caractères de séparation des connexions proxy POP3 génériques:

1. Dans la barre de navigation, sélectionnez **Configuration du téléchargement du courrier**.
2. Spécifiez les nouveaux caractères de séparation que vous souhaitez utiliser (voir “Proxy générique” à la page 29).
3. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Pour spécifier les ports utilisés pour des connexions proxy POP3 dédiées:

1. Dans la page Configuration du téléchargement du courrier (), spécifiez les numéros de ports et les serveurs POP3 dans la liste des connexions proxy dédiées. Vous pouvez spécifier autant de serveurs que vous le souhaitez, mais les numéros de ports qui leur sont associés doivent être uniques (voir “Proxy dédié” à la page 30).

   Pour ajouter un serveur POP3, cliquez sur **Ajouter**, puis indiquez un numéro de port unique (généralement compris entre 1024 et 32767) et le nom de domaine du serveur (par exemple, pop3server.externalorg.com) dans la boîte de dialogue d'ajout qui s'affiche. Cliquez sur **OK** pour l'ajouter à la liste des connexions proxy dédiées.
2. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Configuration de la fonctionnalité de mise à jour automatique

La fonctionnalité de mise à jour automatique maintient le fichier de définition des virus (.DAT) et le moteur d'analyse à jour, garantissant une parfaite protection contre les virus.

IMPORTANT : Lorsque l'application recherche des virus (en fonction des paramètres que vous avez définis), elle utilise le moteur d'analyse des virus et le fichier.DAT en cours pour rechercher et supprimer les virus. De nombreux virus sont découverts tous les jours; c'est pourquoi McAfee crée de nouveaux fichiers de définition pour fournir une protection contre ces nouveaux virus. En outre, de nouvelles versions du moteur d'analyse des virus sont également créées.

Pour configurer la fonctionnalité de mise à jour automatique:

1. Dans la barre de navigation, sélectionnez **Mise à jour automatique de l'Antivirus**.
2. Dans le panneau Site de téléchargement FTP, spécifiez l'emplacement à partir duquel le fichier.DAT et le moteur d'analyse sont copiés. Par défaut, l'application obtient le fichier.DAT et le moteur d'analyse depuis le serveur FTP de Network Associates (ftp.nai.com).

   Pour utiliser un autre serveur FTP, modifiez les zones de texte suivantes:

   - **Nom du serveur**
   - **Chemin d'accès aux fichiers.DAT/moteur**
   - **Nom d'utilisateur du serveur** (si nécessaire)
   - **Mot de passe** (si nécessaire)

   Si votre connexion doit passer par un serveur proxy, fournissez les informations relatives au serveur dans les zones de texte suivantes:

   - **Serveur proxy**
   - **Numéro du port proxy**
   - **Utilisateur du Proxy** (si nécessaire)
   - **Mot de passe du Proxy** (si nécessaire)

   Pour plus d'informations sur la configuration de cette page, affichez la rubrique d'aide correspondante en cliquant sur le bouton d'aide .
3. Cliquez sur **Planning de mise à jour FTP** et sélectionnez les jours et heures (format 24 heures) auxquels vous voulez que l'application mette à jour le fichier.DAT et le moteur d'analyse.

4. Cliquez sur **Appliquer toutes les modifications**.

   Le navigateur Web envoie vos modifications à l'application.

Configuration des autres équipements

Cette section fournit une présentation des modifications que vous devez apporter à vos autres équipements pour intégrer parfaitement l'application dans votre réseau existant. Les modifications varient selon que vous utilisez l'application en mode proxy ou en mode transparence:

- **Mode proxy** (proxy explicite) — Vous devez configurer le reste de votre équipement pour router les protocoles via l'application, afin que rien ne puisse contourner l'application. Cela inclut la configuration de tous vos clients internes (tels que les logiciels HTTP, FTP et POP3) pour qu'ils utilisent l'application comme serveur proxy. Vous devez notamment vous assurer que les paramètres HTTP, FTP et Gopher de vos clients Web sont configurés pour utiliser le numéro de port HTTP. Voir "Routage des protocoles via l'application," ci-dessous.
- **Mode transparence** (proxy transparent) — Par définition, le mode transparence permet d'insérer l'application dans le réseau sans nécessiter une reconfiguration importante des autres équipements. Cependant, il est toujours nécessaire de configurer votre système de messagerie SMTP pour que le trafic de courrier électronique puisse passer via l'application. Voir "Modification des enregistrements du serveur DNS" à la page 54.

IMPORTANT : Au cours de l'utilisation quotidienne de votre système de messagerie, vous devrez peut-être mettre le serveur de messagerie hors ligne afin d'effectuer des changements de configuration ou d'autres tâches de maintenance. Vous devez savoir que si vous laissez l'application en cours d'exécution, elle continuera d'accepter et d'analyser les messages électroniques entrants mais ne sera pas à même de les transmettre (à moins que votre configuration de messagerie n'inclue un serveur de sauvegarde). Si l'application est autorisée à recopier les messages vers le haut, elle risque d'être saturée. Pour éviter ce problème, désactivez le serveur proxy SMTP au niveau de l'application lorsque le serveur de messagerie est hors ligne. Votre firewall retournera alors les messages entrants sous forme de messages non remis.

Routage des protocoles via l'application

Pour plus d'informations sur la configuration des options requises, consultez la documentation accompagnant vos autres équipements. Lorsque vous avez terminé la configuration de l'équipement, vous pouvez exécuter différents tests de la page 55 afin de vous assurer que votre configuration de messagerie est correcte. L'application utilise les ports par défaut suivants pour les protocoles:

- Messagerie électronique (SMTP): 25
- Transfert de fichiers (FTP): 21
- Navigation Web (HTTP): 80
- Téléchargement du courrier (POP3): 110

Si vous avez configuré l'application pour qu'elle utilise des ports différents pour les protocoles, vous devez régler le reste de votre équipement pour qu'il utilise ces ports en conséquence.

Nous vous recommandons également de configurer votre pare-feu pour qu'il envoie et reçoive uniquement du trafic interne de l'application (pour les protocoles traités comme proxy par l'application).

Modification des enregistrements du serveur DNS

Selon la topologie du réseau de votre entreprise et les protocoles que l'application traite comme proxy, vous devrez peut-être modifier des enregistrements des serveurs DNS internes et externes; voir les scénarios présentés au chapitre 1 du Guide produit.

En particulier, si vous avez des serveurs FTP, Web ou POP3, vous devrez peut-être créer des enregistrements pour des serveurs DNS *externes* correspondant aux serveurs FTP, Web et POP3 internes vers votre pare-feu. Pour un serveur Web interne, vous devrez également créer des enregistrements pour le serveur DNS *interne* correspondant au nom de domaine du serveur Web vers son adresse IP.

Les enregistrements inclus au niveau du serveur DNS (et leur ordre) déterminent également si vous mettez en oeuvre une configuration de basculement, de fermeture ou de sécurité intégrée en cas de défaillance (voir le chapitre 1 du Guide produit), aussi devez-vous vous assurer que ces enregistrements sont correctement répertoriés.

Pour plus d'informations sur la modification de votre logiciel de serveur DNS, reportez-vous à la documentation qui l'accompagne.

Tester votre configuration

Nous vous recommandons d'effectuer les tests suivants (selon les serveurs proxy que vous avez activés) afin de vérifier la bonne intégration de l'application WebShield e500 à votre réseau:

- "Test 1: Vérifier que les messages électroniques (SMTP) sont correctement analysés et délivrés" à la page 56.
- "Test 2: Vérifier que les transferts de fichiers (FTP) sont correctement analysés" à la page 57.
- "Test 3: Vérifier que la navigation Web (HTTP) est correctement analysée" à la page 57.
- "Test 4: Vérifier que les téléchargements de courrier (POP3) sont correctement analysés" à la page 58.

Ces tests utilisent un fichier de test spécifique mis au point par le European Institute of Computer Anti-virus Research (EICAR), qui regroupe les principaux fabricants d'antivirus en Europe.

IMPORTANT : Le fichier de test EICAR *ne contient aucun virus* — il ne peut en aucun cas se propager ou infecter d'autres fichiers, ni endommager votre système de quelque façon que ce soit. Lorsque vous aurez terminé votre test, supprimez ce fichier afin que les utilisateurs non avertis n'en soient pas inutilement alarmés.

Vérifiez que vous avez désactivé le logiciel antivirus sur l'ordinateur que vous utilisez pour créer le fichier de test EICAR, afin que votre logiciel antivirus ne supprime pas le fichier de test.

Pour créer le fichier de test EICAR:

1. Ouvrez un éditeur de texte classique, par exemple le Bloc-notes de Microsoft.
2. Si nécessaire, créez un nouveau fichier texte, puis tapez la ligne suivante:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
   ANTIVIRUS-TEST-FILE!$H+H*
   ```

   REMARQUE : La ligne affichée ci-dessus doit tenir sur une seule ligne de la fenêtre de votre éditeur de texte.

3. Enregistrez le fichier texte sous le nom EICAR.COM. La taille du fichier est d'environ 70 octets.

Test 1: Vérifier que les messages électroniques (SMTP) sont correctement analysés et délivrés

Vous pouvez tester l'analyse des virus et la remise de courrier SMTP de votre application en faisant circuler le fichier de test EICAR entre des comptes de messagerie (Internet) internes et externes.

Pour vérifier que l'analyse des virus et la remise de courrier SMTP fonctionne correctement:

1. Ouvrez une session sur un ordinateur de votre réseau disposant d'un compte de messagerie.
2. Créez le fichier de test EICAR.
3. Ouvrez le programme de messagerie de votre ordinateur et créez un nouveau message avec les attributs suivants: spécifiez le destinataire prévu sous la forme d'une adresse électronique externe sur Internet à laquelle vous avez accès, puis joignez le fichier EICAR au message.
4. Envoyez le message.

   Si votre système de messagerie est correctement configuré, et que l'application comporte les paramètres par défaut:

   - le serveur de messagerie reçoit le message sortant de l'ordinateur interne, puis le délivre à l'application.
   - L'application analyse le message à la recherche de virus, détecte le fichier test EICAR joint et le supprime. Elle retourne ensuite le message nettoyé au compte de messagerie interne.
5. Vérifiez que le message a bien été retourné et qu'il ne contient plus le fichier de test EICAR.
6. Accédez au compte de messagerie Internet que vous avez spécifié pour le premier message, et envoyez un message similaire au compte de messagerie interne en y joignant un nouveau fichier de test EICAR.

   Si votre système de messagerie est correctement configuré et si l'application comporte les paramètres par défaut, l'application reçoit le message de réponse. Elle analyse le message à la recherche de virus, détecte le fichier test EICAR joint et le supprime. Elle retourne ensuite le message nettoyé au compte de messagerie externe.
7. Vérifiez que le message a bien été retourné et qu'il ne contient plus le fichier de test EICAR.
8. Supprimez les fichiers de test EICAR que vous avez créés.

Test 2: Vérifier que les transferts de fichiers (FTP) sont correctement analysés

Vous pouvez tester l'analyse de virus FTP de votre application en plaçant le fichier de test EICAR sur un serveur FTP, puis en essayant de le télécharger.

Pour vérifier que l'analyse des virus FTP fonctionne correctement:

1. Ouvrez une session sur le serveur FTP.
2. Créez le fichier de test EICAR.
3. Ouvrez une session sur un ordinateur de votre réseau disposant d'un client FTP (logiciel FTP).
4. Ouvrez le client FTP de l'ordinateur et connectez-vous au serveur FTP.
5. Localisez le fichier de test EICAR et essayez de le télécharger.

   Si votre système FTP est correctement configuré, l'application détecte le fichier de test EICAR et bloque le téléchargement.
6. Supprimez le fichier de test EICAR que vous avez créé.

Test 3: Vérifier que la navigation Web (HTTP) est correctement analysée

Vous pouvez tester l'analyse des virus HTTP de votre application en référençant le fichier de test EICAR à partir d'une page Web sur un serveur Web, puis en essayant de le télécharger.

Pour vérifier que l'analyse des virus HTTP fonctionne correctement:

1. Ouvrez une session sur le serveur Web.
2. Créez le fichier de test EICAR et référencez-le à partir d'une page Web.
3. Ouvrez une session sur un ordinateur de votre réseau disposant d'un client HTTP (navigateur Web).
4. Ouvrez le client HTTP de l'ordinateur et accédez à la page Web comportant le fichier de test EICAR.
5. Essayez de télécharger le fichier de test EICAR.

   Si votre système HTTP est correctement configuré, l'application détecte le fichier de test EICAR et bloque le téléchargement.
6. Supprimez le fichier de test EICAR que vous avez créé.

Test 4: Vérifier que les téléchargements de courrier (POP3) sont correctement analysés

Vous pouvez tester l'analyse de virus POP3 de l'application en envoyant le fichier de test EICAR dans un message adressé à un compte de messagerie POP3, puis en essayant de télécharger ce message.

Pour vérifier que l'analyse des virus POP3 fonctionne correctement:

1. Ouvrez une session sur un ordinateur de votre réseau accédant au serveur POP3 sans analyse.
2. Créez le fichier de test EICAR et envoyez-le à un compte de messagerie sur le serveur POP3.
3. Ouvrez une session sur un ordinateur de votre réseau disposant d'un client POP3 (logiciel de téléchargement de courrier POP3).
4. Téléchargez les messages du compte de messagerie POP3 contenant le message avec le fichier de test EICAR.

   Si votre système POP3 est correctement configuré, l'application détecte le fichier de test EICAR et le supprime du message.
5. Vérifiez que le message ne contient pas le fichier de test EICAR.
6. Supprimez le fichier de test EICAR que vous avez créé.

Utilisation de l'application

L'interface utilisateur de l'application (voir page x) a été conçue dans un souci de simplicité d'utilisation, afin de vous aider à rapidement configurer les paramètres de l'application.

A Barre de navigation

La barre de navigation liste les différentes fonctionnalités pouvant être configurées (une flèche ▸ figure en regard de chacune d'elles). Cliquez sur une fonctionnalité pour afficher la page de paramètres correspondante.

B Page

La page affiche les paramètres de la fonctionnalité que vous avez sélectionnée dans la barre de navigation, vous permettant d'afficher et de modifier ces paramètres.

REMARQUE : Les modifications que vous apportez ne sont pas appliquées tant que vous n'avez pas cliqué sur **Appliquer toutes les modifications**.

Chaque page comporte les boutons suivants:

Guide produit — Affiche une version PDF (Portable Document Format) du Guide produit.

Aide — Permet d'accéder à la rubrique d'aide de la page en cours dans une nouvelle fenêtre du navigateur. Les rubriques d'aide contiennent des informations détaillées, y compris des astuces permettant d'optimiser les fonctionnalités de l'application.

Annuler — Annule les modifications apportées à la page *en cours* depuis les dernières modifications appliquées à l'application. Si vous passez à une autre page, le navigateur Web stocke les modifications apportées; c'est pourquoi vous devez utiliser **Annuler toutes les modifications** si vous ne voulez pas que ces modifications soient appliquées.

C Panneau

Certaines pages comportent des panneaux contenant plusieurs champs. Sélectionnez les options de la page pour afficher les panneaux.

D Boutons de contrôle

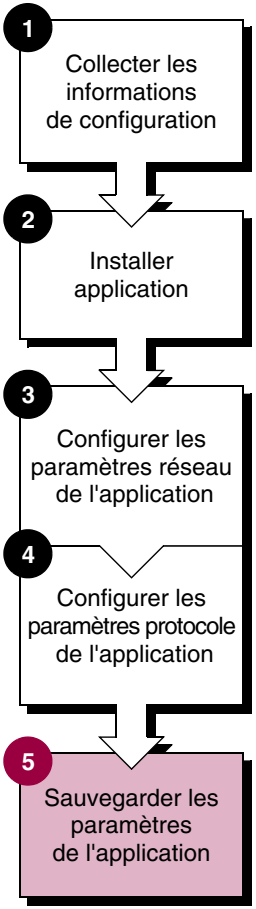
L'interface utilisateur comporte les boutons de contrôle suivants:

- **Déconnexion** — Interrompt la session de gestion en cours. Vous revenez à la page de connexion et devez vous connecter à nouveau avec votre mot de passe pour continuer à gérer l'application.
- **Appliquer toutes les modifications** — Applique les modifications apportées à l'application.
- **Annuler tout**—Annule toutes les modifications apportées à *toutes* les pages depuis la dernière application des modifications à l'application. Si vous avez modifié plusieurs pages, toutes ces modifications sont annulées.

Le présent guide ne fournit pas d'informations détaillées sur la totalité des pages de l'interface utilisateur. Pour obtenir ces informations, reportez-vous aux rubriques d'aide appropriées.

Sauvegarde et restauration de vos paramètres

Lorsque vous avez terminé la configuration des paramètres de l'application, nous vous recommandons de sauvegarder ces paramètres afin de pouvoir rapidement les restaurer, au cas où vous devriez restaurer le logiciel de l'application suite à un problème. La restauration du logiciel de l'application est décrite en détails à la section "Restauration et mise à niveau du logiciel de l'application" à la page 63.



Sauvegarde de vos paramètres

Pour sauvegarder les paramètres de l'application dans un jeu de fichiers de configuration:

1. Ouvrez le navigateur Web depuis l'ordinateur sur lequel vous voulez créer les fichiers de configuration de sauvegarde.
2. Accédez à l'interface utilisateur de l'application à l'aide de l'URL appropriée, et ouvrez une session (voir Etape 2 à la page 36 à Etape 7 à la page 39).
3. Dans la barre de navigation, sélectionnez **Maintenance du système**.
4. Cliquez sur **Enregistrer dans un fichier**, en regard de « Enregistrer les paramètres du système ».

   Une boîte de dialogue Téléchargement de fichier peut apparaître dans votre navigateur, pour vérifier si vous souhaitez télécharger des fichiers à partir de l'application. Si cette boîte de dialogue s'affiche, cliquez sur **OK**.

   La boîte de dialogue Enregistrer sous s'affiche.
5. Sélectionnez l'emplacement de votre choix pour les fichiers de configuration et modifiez le nom du fichier.ZIP le cas échéant. Par défaut, il s'agit du fichier ws_cfg_backup.zip.
6. Cliquez sur **Enregistrer**.

   Le navigateur Web crée les fichiers de configuration. Si la procédure s'est déroulée sans problème, une boîte de dialogue de confirmation s'affiche.
7. Fermez cette boîte.

   Vous pouvez à présent poursuivre la gestion de l'application.

Restauration de vos paramètres

Quand vous restaurez les paramètres de l'application avec un fichier de configuration, vous devez vous assurer que les autres modifications nécessaires sont effectuées. Par exemple, vous pouvez utiliser le même fichier de configuration pour plusieurs applications mais celles-ci ne peuvent pas partager les adresses IP (les adresses IP doivent être uniques) et vous devez donc modifier en conséquence les adresses IP.

L'application peut utiliser les fichiers de configuration générés par une version antérieure de l'application. En conséquence, si vous avez généré un tel fichier avant de mettre à niveau votre application, vous pouvez simplement utiliser le fichier de configuration pour restaurer vos paramètres antérieurs à la mise à niveau de l'application.

Pour restaurer les paramètres de l'application à partir d'un jeu de fichiers de configuration:

1. Ouvrez le navigateur Web sur l'ordinateur contenant les fichiers de configuration, puis accédez à l'interface utilisateur de l'application à l'aide de l'URL appropriée et connectez-vous (voir Etape 2 à la page 36 à Etape 7 à la page 39).

   Si vous accédez à l'interface utilisateur de l'application, mais que les fichiers de configuration se trouvent sur un autre ordinateur, transférez les fichiers sur le premier ordinateur.

2. Selon la configuration que vous appliquez à l'application, effectuez l'une des actions suivantes:

   - Si vous avez récemment mis à jour le logiciel de l'application ou que vous configurez celle-ci pour la première fois, la page Configuration du système contient un panneau supplémentaire intitulé Restaurer la configuration. Cliquez sur **Restaurer la configuration** (sur la page Configuration du système) pour accéder au panneau.

     ☐ **REMARQUE :** Le panneau Restaurer la configuration n'est disponible sur le panneau Configuration du système que lors de la première configuration de l'application.

   - Si vous avez déjà configuré l'application, sélectionnez **Maintenance du système** (dans la barre de navigation) pour afficher la page Maintenance du système. Regardez les zones de texte **Fichier** et **URL** situées à côté de « Restaurer les paramètres du système ».

3. Dans la zone de texte **Fichier** ou **URL**, indiquez le chemin d'accès complet ou l'URL des fichiers de configuration. Exemples:

   ```
   c:\myfiles\ws_cfg_backup.zip
   ```

   ```
   http://www.myorg.com/myfiles/ws_cfg_backup.zip
   ```

   Vous pouvez cliquer sur **Parcourir** pour localiser le fichier.

4. Cliquez sur **Restaurer maintenant**.

   Le navigateur Web ouvre les fichiers de configuration et envoie les paramètres à l'application. Vous pouvez à présent poursuivre la gestion de l'application.

Restauration et mise à niveau du logiciel de l'application

Si un problème survient au niveau d'une unité de disque dur de l'application, vous pouvez la remplacer par une autre unité (aux spécifications identiques) alors que l'application est en cours de fonctionnement: l'application copie l'image à partir de l'unité existante sur l'unité de remplacement; voir page 69.

Cependant, certaines circonstances peuvent nécessiter la restauration du logiciel de l'application sur les deux unités. Bien que cette situation soit improbable, elle peut se produire si vous retirez simultanément les deux unités de l'application. Le processus de restauration requiert l'emploi du CD-ROM de récupération de l'application WebShield e500.

Vous recevrez peut-être un CD-ROM de mise à jour de l'application WebShield e500 du représentant du support technique, CD contenant des améliorations logicielles pour l'application. La mise à niveau des unités de l'application à partir de ce CD-ROM se déroule de façon similaire au processus de restauration.

❑ **REMARQUE :** Vous devez vous connecter localement à l'application lorsque vous restaurez ou mettez à niveau son logiciel. Vous ne pouvez pas effectuer de restauration ou de mise à niveau à distance.

Lors de la restauration du logiciel de l'application, le processus de restauration supprime tout logiciel supplémentaire que vous avez installé. Si vous utilisez ePolicy Orchestrator avec l'application, vous devrez réinstaller l'agent ePolicy Orchestrator à l'issue du processus de restauration; voir le Guide de configuration.

Pour restaurer ou mettre à niveau le logiciel de l'application:

1. Connectez un clavier au port clavier de l'application (de couleur violette, voir F page 16).
2. Connectez un écran au port écran de l'application (voir G page 16).
3. Allumez l'application si elle est éteinte.
4. Insérez le CD-ROM de récupération ou le CD-ROM de mise à niveau de l'application WebShield e500 dans l'unité de CD-ROM (voir B page 14). Le CD-ROM utilisé est différent selon que vous restaurez ou mettez à niveau le logiciel.
5. Appuyez sur le bouton de réinitialisation du panneau de contrôle, situé à l'avant de l'unité (voir C page 15).

   L'application exécute sa séquence d'amorçage. Elle lit ensuite le CD-ROM et affiche un contrat de licence.

   ☐ **REMARQUE :** La procédure suivante correspond à l'utilisation du CD-ROM de récupération de l'application WebShield e500. Toutefois, si les invites qui s'affichent sont différentes de celles de votre CD-ROM, suivez les messages à l'écran.

   ---

6. Lisez attentivement l'accord de licence, puis tapez `Y` pour l'accepter.

   Si vous n'acceptez pas l'accord de licence — tapez `N` pour le refuser — vous ne pouvez pas utiliser le logiciel qui se trouve sur le CD-ROM.

   Les options suivantes sont présentées:

   1: Exécution d'une installation complète supprime toutes les données des unités de disque dur de l'application et réinstalle le logiciel.

   2: Installation du logiciel du CD-ROM réinstalle le logiciel tout en essayant de conserver les zones contenant les éléments suivants:

   - Données de la configuration
   - Données des fichiers journal
   - Messages électroniques mis en quarantaine
   - Messages électroniques différés

   Si le processus de restauration ne peut pas préserver ces zones, il les recrée.

3: Exécution d'une mise à niveau logicielle effectue les mises à niveau logicielles appropriées (si disponibles) figurant sur le CD-ROM.

4: Opération automatique détermine laquelle des trois options ci-dessus est appropriée et l'exécute.

5: Exécution d'une installation complète et arrêt supprime toutes les données des unités de disque dur de l'application et réinstalle le logiciel. Après l'installation, l'application éjecte le CD-ROM mais ne redémarre pas. Vous pouvez alors éteindre l'application.

6: Rétablir les mots de passe par défaut rétablit le mot de passe par défaut de l'application, à savoir `e500changeme`.

7: Ne rien faire et redémarrer laisse l'application inchangée et éjecte le CD-ROM. Choisissez cette option si vous avez inséré le CD-ROM par erreur et ne souhaitez pas restaurer ou mettre à niveau le logiciel de l'application.

7. Entrez le nombre correspondant à l'option requise.

   Vous êtes invité à indiquer si vous souhaitez poursuivre.

8. Entrez `Y`.

   A moins que vous n'ayez choisi l'option **7: Ne rien faire et redémarrer**, le processus de restauration ou de mise à niveau débute. Un écran d'état indique la progression du processus. Selon l'option que vous avez sélectionnée, le processus peut durer jusqu'à 30 minutes.

AVERTISSEMENT : Selon l'option choisie, l'application peut revenir aux paramètres par défaut, perdant ainsi les paramètres de configuration que vous aviez définis.

Lorsque le processus de restauration ou de mise à niveau est achevé, l'application éjecte le CD-ROM puis redémarre (sauf si vous avez choisi l'option **5: Exécution d'une installation complète et arrêt**). Une fois la séquence d'amorçage terminée (après environ deux minutes), l'application est opérationnelle. Selon l'option que vous avez sélectionnée, vous devrez peut-être reconfigurer les paramètres de l'application; voir page 35.

☐ **REMARQUE :** Lorsque vous accédez à l'application et ouvrez une session, vous devez savoir que les modifications suivantes peuvent s'être produites si vous avez choisi de ne pas conserver les paramètres précédents (ou si ceux-ci n'ont pas pu être conservés):

- Le mot de passe est de nouveau le mot de passe par défaut, à savoir `e500changeme`.
- Le port de données est revenu à l'adresse IP par défaut, 10.1.1.108.
- Le port de gestion est activé et l'adresse IP par défaut, 10.1.2.108, a été rétablie.

Voir l'annexe A du Guide produit pour plus d'informations sur les paramètres par défaut de l'application.

Dépannage

Problèmes matériels

Cette section contient des solutions aux problèmes que vous pouvez rencontrer lors de l'installation et de l'exécution de l'application. Pour des solutions concernant les problèmes liés à l'interface utilisateur, voir page 70.

L'application n'est pas alimentée

Vérifiez les points suivants:

- L'application est correctement branchée, à l'aide du cordon d'alimentation fourni, sur une prise électrique en état de marche.
- Le bouton de marche/arrêt et le bouton de mise sous tension sont tous deux en position de marche ; voir Etape 6 à la page 34.

  Le bouton de mise sous tension se trouve à l'arrière de l'unité (voir E page 16). Le bouton de marche/arrêt se trouve sur le panneau de contrôle, à l'avant de l'unité (voir C page 15).

Si l'application ne reçoit toujours pas de courant, vérifiez la prise électrique en y branchant un autre appareil. Si elle fonctionne, il y a un problème au niveau de l'application ou de son cordon d'alimentation. Contactez votre fournisseur.

L'application ne reçoit aucun trafic en provenance du réseau

Vérifiez les points suivants:

- L'application est sous tension et son logiciel est en cours d'exécution: le voyant d'alimentation est allumé (sur le panneau de contrôle, voir C page 15) et le voyant du disque dur est éteint (voir A page 14).
- Le câble réseau que vous utilisez n'est pas endommagé et est correctement connecté aux ports de l'application et à l'équipement réseau existant. Si vous n'avez pas utilisé les câbles bleus fournis avec l'application, vérifiez que ceux que vous utilisez sont bien des câbles réseau Cat 5 (catégorie 5) UTP «direct» (non croisé).
- Vous avez connecté le port réseau local 2 à l'équipement réseau existant, si si vous utilisez l'application en mode transparence.

Si l'application ne reçoit toujours pas de trafic, vérifiez les câbles réseau et les ports réseau de votre équipement réseau existant. Si les câbles et les ports fonctionnent, il y a un problème au niveau de l'application. Contactez votre fournisseur.

Le voyant d'une unité de disque dur est rouge

Le disque dur est défectueux et doit être remplacé.

Les unités se trouvent sur des chargeurs, ce qui permet de remplacer une unité défaillante alors que l'application fonctionne. L'image de l'unité de remplacement est automatiquement créée à partir de l'unité existante.

AVERTISSEMENT : Lorsque vous remplacez des unités de disque dur, veillez à respecter les indications suivantes :

- Ne retirez pas les deux unités de l'application en même temps. Il doit toujours y avoir au moins une unité dans l'application.
- Ne laissez pas l'application fonctionner plus de quelques minutes avec une seule unité : cela perturbe le système d'aération et risque de provoquer une surchauffe. Insérez immédiatement l'unité de remplacement.
- Utilisez uniquement des unités dont les spécifications sont parfaitement identiques à celles des unités existantes.
- Lors de la manipulation des unités, veillez à ne pas toucher de composant sensible à l'électricité statique. Prenez des précautions raisonnables pour éviter toute décharge d'électricité statique et ne mettez pas la main ou un objet dans le logement vide de l'unité.

Pour remplacer une unité défectueuse:

1. Appuyez sur le bouton d'éjection de l'unité défectueuse, puis abaissez la poignée (Figure 3-5). Sortez l'unité de son logement.

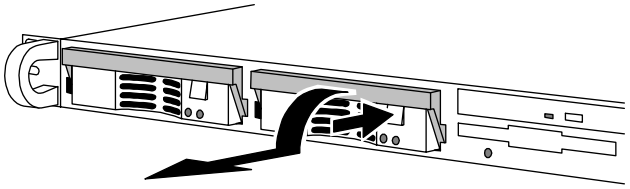


Figure 3-5. Retrait de l'unité

2. Faites glisser l'unité de remplacement dans le logement vide, puis remontez la poignée afin de verrouiller l'unité en place (Figure 3-6).

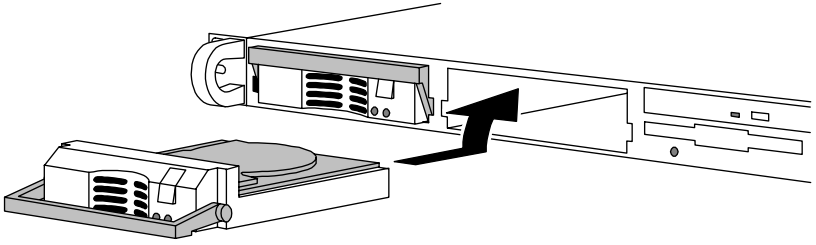


Figure 3-6. Insertion de l'unité

L'application copie l'image sur l'unité de remplacement à partir de l'unité existante. Cette opération peut durer de 20 à 30 minutes. Tout au long de l'opération, le voyant vert de l'unité de remplacement clignote.

Les voyants des deux unités de disque dur sont rouges

Il y a un problème au niveau des unités de l'application. Utilisez le CD-ROM de récupération de l'application WebShield e500 pour restaurer le logiciel; voir page 63. Si l'application ne fonctionne toujours pas, contactez votre fournisseur.

Problèmes d'interface utilisateur

Cette section contient des solutions aux problèmes que vous pouvez rencontrer lors de la configuration de l'application via l'interface utilisateur.

Impossible d'accéder à la page « Connexion »

Vérifiez les points suivants:

- L'application est sous tension et son logiciel est en cours d'exécution: le voyant d'alimentation est allumé (sur le panneau de contrôle, voir C page 15) et le voyant du disque dur est éteint (voir A page 14).
- Vous avez tapé `https` (au lieu de `http`) dans le champ URL de votre navigateur Web. Vérifiez que votre navigateur prend en charge le cryptage SSL (Secure Sockets Layer) v3.0 et qu'il est activé.
- L'application ne doit pas être configurée en tant que serveur proxy de l'ordinateur de gestion (ordinateur utilisé pour gérer l'application). Si un serveur proxy se trouve entre l'ordinateur de gestion et l'application, il doit être configuré en tant qu'hôte de remise de l'application.
- Si vous êtes connecté à distance à l'application (par le réseau) via le port réseau local 1 (voir H page 17), vérifiez que:
  - L'ordinateur que vous utilisez dispose d'une connexion active au réseau et qu'il peut atteindre le même sous-réseau que celui auquel l'application est connectée.
  - Vous avez utilisé la nouvelle adresse IP que vous avez configurée pour le port réseau local 1, dans le champ URL de votre navigateur Web. Si vous n'avez pas désactivé ou supprimé l'adresse IP par défaut `10.1.1.108`, essayez d'utiliser cette adresse (`https://10.1.1.108`).

    L'adresse IP de l'application doit être compatible avec le sous-réseau auquel l'application est connectée. Si ce n'est pas le cas, essayez d'utiliser l'adresse IP par défaut et, en cas d'échec, essayez une connexion de gestion directe; voir Etape 4 à la page 32.

    ☐ **REMARQUE :** Vous ne pouvez obtenir une connexion de gestion directe via le port réseau local 2 que si vous utilisez l'application en mode proxy *et* que vous n'avez pas désactivé le port réseau local 2 (Etape 17 à la page 41).

– L'application possède une connexion valide au réseau existant: le voyant d'activité réseau NIC 1 (carte réseau 1) clignote (sur le panneau de contrôle, voir C page 15).

Si le voyant ne clignote pas, vérifiez que le câble que vous utilisez n'est pas endommagé et est correctement connecté au port de données de l'application et au reste de votre équipement réseau. Si vous n'avez pas utilisé le câble bleu fourni avec l'application, vérifiez que celui que vous utilisez est bien un câble réseau Cat 5 (catégorie 5) UTP « direct » (non croisé).

- Si l'application fonctionne en mode proxy et que vous avez une connexion de gestion locale directe via le port LAN2 (voir I page 18), vérifiez que:

  – Vous n'avez pas désactivé le port LAN2. Pour vérifier ce point, vous devez vous connecter à distance.

  – Vous avez utilisé la nouvelle adresse IP que vous avez configurée pour le port LAN2 (l'adresse IP par défaut est `10.1.2.108`), dans le champ URL de votre navigateur Web.

  – L'application possède une connexion valide à votre ordinateur: le voyant d'activité réseau NIC 2 (carte réseau 2) clignote (sur le panneau de contrôle, voir C page 15).

  Si le voyant ne clignote pas, vérifiez que le câble que vous utilisez n'est pas endommagé et est correctement connecté au port LAN2 de l'application et au port réseau de votre ordinateur. Si vous n'avez pas utilisé le câble orange fourni avec l'application, vérifiez que celui que vous utilisez est bien un câble réseau croisé Cat 5 (catégorie 5) UTP.

La page « Connexion » s'affiche, mais le bouton de connexion indique « Initialisation en cours »

L'application vérifie que votre navigateur Web dispose des composants requis par l'interface utilisateur.

L'application est optimisée pour Internet Explorer version 4.0, 5.0, 5.5 ou 6.0 et prend en charge Netscape Navigator version 4.7. Si vous utilisez un autre navigateur Web, vous ne pourrez peut-être pas accéder à l'interface utilisateur pour configurer l'application.

L'interface utilisateur de l'application nécessite l'utilisation de Java 2 Runtime Environment; il se peut donc que votre navigateur soit en train d'installer ce logiciel. La taille du logiciel Java 2 Runtime Environment est de 5 à 14 Mo (selon les composants requis par votre navigateur) et son installation peut prendre du temps si votre liaison distante à l'application est peu rapide.

Mon mot de passe ne fonctionne pas

Si vous avez récemment restauré le logiciel de l'application sans conserver les paramètres précédents, le mot de passe est de nouveau le mot de passe par défaut, à savoir `e500changeme`.

J'ai oublié mon mot de passe

Vous devez utiliser le CD-ROM de récupération de l'application WebShield e500 pour revenir au mot de passe par défaut `e500changeme` ; voir "Restauration et mise à niveau du logiciel de l'application" à la page 63. Utilisez l'option **6 : Rétablir les mots de passe par défaut** lors du processus de restauration.

Une partie de l'interface utilisateur ne s'affiche pas correctement

L'interface utilisateur de l'application est optimisée pour Microsoft Internet Explorer version 4.0, 5.0, 5.5 ou 6.0 et prend en charge Netscape Navigator version 4.7. Vérifiez les notes de version jointes pour voir s'il existe des problèmes connus lors de l'utilisation de certains navigateurs Web sur des systèmes d'exploitation particuliers.

Mes clients (logiciels) ne peuvent pas communiquer via l'application

Vérifiez les points suivants:

- Les serveurs proxy sont activés pour l'application (par défaut, tous les protocoles pris en charge sont activés) ; voir "Configuration des protocoles de l'application" à la page 46.
- Les clients et autres équipements sont configurés pour acheminer le trafic vers et depuis l'application ; voir "Configuration des autres équipements" à la page 53.
- Il n'y a pas de problème au niveau du réseau et votre équipement est correctement connecté.

Le navigateur Web ne fonctionne pas, ou bien le blocage d'URL n'est pas appliqué

L'application doit disposer d'un accès à un serveur DNS pour vérifier les demandes de navigation Web (HTTP) et déterminer quelle URL bloquer si le blocage d'URL est configuré. C'est pourquoi vous devez configurer un serveur DNS à la page Configuration du système ; voir Etape 9 à la page 39.

インストール ガイド — 日本語

概要

このインストール ガイドには、WebShield アプライアンスのインストールと構成に必要な情報が記載されています。詳細については、以下のセクションを参照してください。

著作権と商標 **2 ページ**

電源および安全に関する情報 **3 ページ**

WebShield e500 アプライアンスについて **5 ページ**

- 製品の特色 6 ページ
- パッケージの内容 10 ページ

アプライアンスの準備 **13 ページ**

- インストールに必要なスキル 13 ページ
- ポートとコネクタ 14 ページ
- 設定情報の収集 19 ページ

アプライアンスのインストール **31 ページ**

ネットワーク構成の設定 **35 ページ**

プロトコルの設定 **43 ページ**

- プロトコルの設定 44 ページ
- 自動アップデートの設定 50 ページ
- 他の機器の設定 51 ページ
- 設定のテスト 53 ページ

アプライアンスの使用方法 **57 ページ**

- 設定のバックアップと復元 59 ページ
- ソフトウェアの復元とアップグレード 61 ページ

トラブルシューティング **65 ページ**

- ハードウェアに関する問題 65 ページ
- ユーザ インターフェースに関する問題 67 ページ

著作権と商標

著作権
© 2001-2002 Networks Associates Technology, Inc. All Rights Reserved. このマニュアルのいかなる部分も、Network Associates Technology, Inc. またはその代理店または関連会社の書面による許可なしに、形態、方法を問わず、複写、送信、転載、検索システムへの保存、および他言語に翻訳することを禁じます。許諾を得る際には、下記の Network Associates 法務部門まで書面にてご連絡ください。3965 Freedom Circle, Santa Clara, California 95054 もしくは call +1-972-308-9960.

登録商標及び商標

Active Security、*Active Security (in Katakana)*、*ActiveHelp*、*ActiveShield*、*AntiVirus Anyware and design*、*Bomb Shelter*、*Certified Network Expert*、*Clean-Up*、*CleanUp Wizard*、*CNX*、*CNX Certification Certified Network Expert and design*、*CyberCop*、*CyberCop (in Katakana)*、*CyberMedia*、*CyberMedia UnInstaller*、*Design (stylized N)*、*Disk Minder*、*Distributed Sniffer System*、*Distributed Sniffer System (in Katakana)*、*Dr Solomon's*、*Dr Solomon's label*、*Enterprise SecureCast*、*Enterprise SecureCast (in Katakana)*、*EZ SetUp*、*First Aid*、*ForceField*、*GMT*、*GroupShield*、*GroupShield (in Katakana)*、*Guard Dog*、*HelpDesk*、*HomeGuard*、*Hunter*、*ISDN TEL/SCOPE*、*LANGuru*、*LANGuru (in Katakana)*、*M and design*、*Magic Solutions*、*Magic Solutions (in Katakana)*、*Magic University*、*MagicSpy*、*MagicTree*、*McAfee*、*McAfee (in Katakana)*、*McAfee and design*、*MultiMedia Cloaking*、*Net Tools*、*Net Tools (in Katakana)*、*NetCrypto*、*NetOctupus*、*NetScan*、*NetShield*、*NetStalker*、*Network Associates*、*NetXray*、*NotesGuard*、*Nuts & Bolts*、*Oil Change*、*PC Medic*、*PC Medic 97*、*PCNotary*、*PGP*、*PGP (Pretty Good Privacy)*、*Pretty Good Privacy*、*PrimeSupport*、*Recoverkey*、*Recoverkey – International*、*Registry Wizard*、*ReportMagic*、*RingFence*、*Router PM*、*SalesMagic*、*SecureCast*、*Service Level Manager*、*ServiceMagic*、*SmartDesk*、*Sniffer*、*Sniffer (in Hangul)*、*SniffMaster*、*SniffMaster (in Hangul)*、*SniffMaster (in Katakana)*、*SniffNet*、*Stalker*、*SupportMagic*、*TIS*、*TMEG*、*TNV*、*TVD*、*TNS*、*Total Network Security*、*Total Network Visibility*、*Total Network Visibility (in Katakana)*、*Total Service Desk*、*Total Virus Defense*、*Trusted Mail*、*UnInstaller*、*Virex*、*Virus Forum*、*ViruScan*、*VirusScan*、*WebScan*、*WebShield*、*WebShield (in Katakana)*、*WebSniffer*、*WebStalker*、*WebWall*、*Who's Watching Your Network*、*WinGauge*、*Your E-Business Defender*、*ZAC 2000*、*Zip Manager* は米国法人 Network Associates, Inc. またはその関係会社の米国またはその他の国における登録商標です。本書中のその他の登録商標及び商標はそれぞれその所有者に帰属します。

ライセンス条項

お客様へ：お客様がお買い求めになられたライセンスに従い、該当する契約書（許諾されたソフトウェアの使用につき一般条項を定めるものです、以下「本契約」といいます）をよくお読みください。お買い求めになられたライセンスタイプがご不明の場合には、担当営業またはライセンス付与管理部門にご相談になるか、製品に付随する購入関係書類若しくは購入手続きにおいて別途受領された書類をご参照ください。本契約の規定に同意されない場合は、製品をインストールしないで下さい。（この場合ご購入元に速やかにご返品いただければ、所定の条件を満たすことによりご購入額全額をお返しできる場合があります。）

電源および安全に関する情報

重要：WebShield e500 アプライアンスを安全にご使用頂くため、アプライアンスを設置する前に、以下の情報をよくお読みください。

電源要件

- 国で定められた規格に準拠している電源コードを使用してください。コードが適合していない場合はご購入先までお問い合わせください。電源コードは改造しないでください。
- アプライアンスを接続するコンセントは、ご使用になる国の電気規格に適合していなければなりません。
- アプライアンスをコンセントや他の機器に接続する際は、転倒事故を防止するため、必ずケーブルを収容し、安全にまとめてください。

使用上の注意

- アプライアンス本体のカバーは開けないでください。製品内部にユーザがメンテナンスできる部品はありません。
- アプライアンスには重量があります。持ち運ぶ際には、ケガをしたり、アプライアンスが損傷したりしないよう、しっかりと持ち、慎重に運んでください。
- アプライアンスは机などの平らな面に置くか、19 インチ ラックのようなラックで安全に保護してください。設置場所がアプライアンスの重量に対応し、落ちないことを確認してください。
- アプライアンスの上に重いものを載せないでください。
- アプライアンスのネットワーク ポートはRJ-45コネクタのみに対応しています。アプライアンスを電話用の差込口に接続しないでください。ただし、接続しようとしている電話線のソケットが 10Mbps または 100Mbps の Ethernet ネットワークに使用されている場合を除きます。
- 万一、アプライアンスのハードウェアに障害が起きた場合には、アプライアンスの電源を切り、電源コードをプラグから抜いてください。ご購入先にご連絡ください。

稼動条件

- 製品を使用する環境が、標準的なコンピュータの使用に適していることを確認してください。風通しがよく湿度が高くないことを確認してください。稼動時は、気温を 10 ～ 40 ℃に、湿度は 90% 以内に保ってください。この範囲を超えると、アプライアンスが正しく動作しない場合があります。
- 製品の使用時は、本体の後方に最低でも 1 インチ（25mm）の隙間を空けてください。これにより製品が適切に冷却されます。
- 製品の通気孔やファン　グリルから液体やその他の異物を入れないでください。

WebShield e500 アプライアンスについて

WebShield e500 アプライアンス（図 4-1）は、強力な WebShield ソフトウェアを搭載している専用のウイルス対策およびコンテンツ スキャン サーバです。このアプライアンスは、Web ブラウザから構成することができます。また、ほとんどのネットワーク トポロジで使用可能です。このアプライアンスでは、次のプロトコルに対してウイルス スキャンを実行します。

- SMTP（Simple Mail Transfer Protocol）の電子メール メッセージ
- FTP（ファイル転送プロトコル）によるファイル転送
- HTTP（Hypertext Transfer Protocol ）による Web ブラウズ
- POP3（Post Office Protocol version 3）によるインターネット電子メール メッセージ

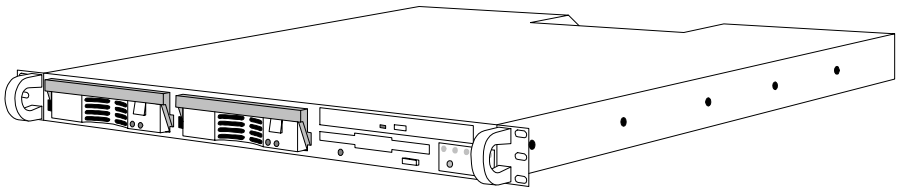


図 4-1. WebShield e500 アプライアンス

このアプライアンスは、コンテンツ スキャン、電子メールの不正中継対策、スパム対策などの機能により、インターネット ゲートウェイを完全に保護し、悪意のあるマテリアルの侵入を防ぎます。

WebShield e500 アプライアンスでは、スキャンするプロトコル間でリソースを共有し、必要に応じて送受信トラフィックをチェックします。アプライアンスは、感染した圧縮ファイルやマクロを含む電子メールを検出し、ウイルスの駆除、感染の記録、感染ファイルの隔離を行い、このような電子メールが受信者に送信されないようにします。また、HTTP、FTP、および POP3 で送信された感染アイテムをブロックします。

このアプライアンスでウイルス スキャンを実行することにより、メール サーバを従来どおりメール管理専用として使用することができます。また、複数の WebShield e500 アプライアンスを同時に使用すると、スキャン時のスループットを強化し、耐障害性を向上させることができます。

アプライアンスの使用方法については、『製品ガイド』の第 1 章を参照してください。

製品の特色

透過モード ― バージョン 2.5 の新機能

バージョン 2.5 の WebShield アプライアンスでは、新機能として透過モードが追加されています。このリリースから、アプライアンスをプロキシ モードと透過モードのいずれかで使用できるようになりました。

- **プロキシ モード**（明示プロキシ）は、アプライアンスを経由してプロトコル トラフィックをルーティングするように、ネットワークの装置を簡単に設定することができる場合に適しています。透過モードが導入されるまでは、アプライアンスはプロキシ モードのみで動作していました。

  プロキシ モードの場合、アプライアンスがプロキシングするプロトコルのトラフィックしか処理されません。

- **透過モード**（透過プロキシ）は、装置を設定するのが難しかったり、時間がかかったりする場合に適しています。アプライアンスはネットワーク上で透過的に存在し、静的ルーティング情報や動的ルーティング情報を使用して、スキャンするトラフィックの送受信を行います。

  注意：透過モードでは、アプライアンスの LAN1 ポートと LAN2 ポートは、別々のサブネットに接続していなければなりません。

  アプライアンスは 2 つのサブネット間に流れるすべての IP トラフィックを処理します。

2 つのモードの詳細については、『製品ガイド』の「プロキシ モードと透過モード」を参照してください。

重要：2 つのモードはそれぞれ別のものです。アプライアンスのインストールと設定を行う前に、使用するモードをよく理解したうえで選択してください。

以前のバージョンの設定ファイルを使用してアプライアンスを設定する場合は、60 ページの「設定の復元」を参照してください。

次に、アプライアンスのその他の特色についてご説明します。

ハードウェア

このアプライアンスには次のような特色があります。

- 1U 高さ 19 インチのラックに埋め込み可能なハードウェア
- Intel Pentium III 1GHz デュアル プロセッサ。
- 256MB の PC133 SDRAM。
- RJ-45 10/100Mbps の自動検出式 Ethernet ネットワーク ポートを 2 ポート装備。既存のネットワークへの柔軟な接続を可能とし、専用の管理インターフェースを実現します（プロキシ モードでのみ使用可能）。
- ホット接続が可能な RAID 1（ミラー）仕様の 17.4GB SCSI ハードディスクを 2 機搭載。これにより、一方のディスクで予想外の問題が発生しても、確実にシームレスな処理を行うことができます。代替ドライブの装着時は、RAID コントローラが自動的に新しいディスクをミラーリングしなおします。

ポートとコネクタの詳細については、14 ページを参照してください。

ソフトウェア

このアプライアンスのソフトウェアには次のような特色があります。

- Web ブラウザから SSL（Secure Sockets Layer）暗号化機能を使用した Web 管理を実現します。
- 設定が簡単なユーザ インターフェースが用意されています。これにより、アプライアンスのセットアップをすばやく行うことができます。設定情報が記憶されるため、最小限の操作で設定を完了することができます。
- 複雑な環境でも簡単に設定できる柔軟なプロキシが用意されています。詳細については、19 ページの「設定情報の収集」を参照してください。
- SMTP 電子メール メッセージのウイルス スキャン機能により、ウイルス感染や禁止されているコンテンツをチェックします。この他にも、次のような機能があります。
  - SMTP 電子メール配信を柔軟に設定できます。複数の電子メール配信方法をセットアップし、耐障害性を持たせることができます。
  - メッセージのコンテンツ スキャンを柔軟に設定できます。禁止されているコンテンツを検索し、特定の種類の添付ファイルをブロックします。
  - 送受信者またはサーバによるスパム防止（受け取りたくない電子メール メッセージを拒否します）。

  - ブラックホール リストをリアルタイムにサポートし、スパム メッセージの潜在的なソースを識別します。アプライアンスは、これらのリストを使用して、スパム メッセージをブロックします。ブラックホール リストは、MAPS（Mail Abuse Prevention System）などの多くの組織から提供されています。http://www.mailabuse.org を参照してください。
  - 指定されたサーバまたはドメインから別のサーバにメッセージを中継します。承認されていない送信者がアプライアンスを経由してスパム メール メッセージを送信できないようにする不正中継防止機能もあります。

- FTP のウイルス スキャン機能によって、感染ファイルをスキャンします。
- HTTP Web ブラウズのウイルス スキャンによって、感染したコンテンツをブロックします。Java、ActiveX、スクリプトもブロックできます。
- POP3 電子メール メッセージのウイルス スキャン機能により、感染したファイルをチェックします。
- 送受信トラフィックを個別にスキャンします。各トラフィックに対して別々にスキャン オプションを設定できます。
- McAfee ウイルス定義ファイル（.DAT ファイル）と McAfee スキャン エンジンの自動アップデート スケジュールを個別に設定できます。これにより、常に最新のウイルス スキャンを実行することができます。
- 一般的な圧縮ファイル内のウイルスを検出します。
- 柔軟なスキャン アクションにより、ウイルスの駆除、感染ファイルの削除、ブロック、隔離を行うことができます。
- 隔離領域に電子メール メッセージを隔離して、検査することができます。次のような電子メール メッセージが隔離できます。
  - ウイルスに感染した受信メッセージ
  - ウイルスに感染した送信メッセージ
  - 禁止されたコンテンツを含む受信メッセージ
  - 禁止されたコンテンツを含む送信メッセージ
- ウイルス感染の検出を通知することができます。電子メール、XML ログ、SNMP レポート、ePolicy Orchestrator レポートなど、さまざまな形式でアラートを送信することができます。詳細については、『コンフィグレーション ガイド』を参照してください。

- スキャン アクティビティとプロトコル ストリームの詳細なログが生成されるので、過去のパフォーマンス情報や配信情報を表示することができます。また、ユーザ インターフェースからグラフ、レポート、ログを作成することもできます。
- McAfee ePolicy Orchestrator をサポートします。これにより、アプライアンスと ePolicy Orchestrator サーバを統合し、アプライアンスで記録された情報からグラフィカルで詳細な統計、履歴、および管理レポートを作成することができます。詳細については、『コンフィグレーション ガイド』を参照してください。
- 迅速なバックアップ プロセスにより、ネットワークを介してアプライアンスの設定を保存し、復元することができます。詳細については、59 ページを参照してください。
- 復元プロセスにより、予想外の問題が発生した場合にアプライアンスのソフトウェアを迅速に復元することができます。61 ページを参照してください。

製品使用上の注意

このアプライアンスには多くの機能がありますが、次の点に注意してください。

- アプライアンスはファイアウォールではありません。社内にある既存のファイアウォールの内側で使用してください。
- アプライアンスはメール サーバではありません。アプライアンスを経由してプロトコル トラフィックをルーティングする場合には、ファイアウォール、メール サーバ、Web キャッシュなどの装置を設定する必要があります。51 ページを参照してください。
- アプライアンスはメール転送エージェントではありません。また、電子メールを隔離または保留されない限り、電子メールは保持されません。
- アプライアンスは、Web ページを格納する一般的な Web サーバではありません。
- アプライアンスは、他のソフトウェアやファイルを格納するための一般的なサーバではありません。アプライアンスのマニュアルやサポート担当者からの指示がない限り、アプライアンスにソフトウェアをインストールしたり、ファイルを追加したりしないでください。
- プロキシ モードで処理できるのは、SMTP、FTP、HTTP、POP3 のトラフィックのみです。これ以外のトラフィックをアプライアンス経由でルーティングしないようにしてください。

パッケージの内容

製品パッケージの内容をよく確認し、アプライアンスの付属品一式が揃っているかどうか確認してください。付属品が足りない場合、または損傷している場合は、購入先までご連絡ください。

ハードウェアとソフトウェア

- RJ-45 接続の CAT-5 UTP ネットワーク ケーブル 3 本
  - 2 本の青いケーブルはストレート ケーブルです（クロスケーブルではありません）。
  - オレンジ色のケーブルはクロスケーブルです。

  これらのケーブルの使用方法は、31 ページの「アプライアンスのインストール」に記載されています。
- マウンティング キット。アプライアンスを 19 インチのラックに組み込みます。
- WebShield e500 アプライアンス復旧 CD
- 各国に対応するさまざまな電源コード

> **重要：**国で定められた規格に準拠している電源コードを使用してください。コードが適合していない場合はご購入先までお問い合わせください。アプライアンスを電源に接続する前に、必ず3 ページの「電源および安全に関する情報」を参照してください。

製品マニュアル

このアプライアンスに付属のマニュアルはこのガイドだけです。他のマニュアルについては、『リリース ノート』を参照してください。

他の資料

- 保証書とユーザ登録カード
- McAfee PrimeSupport 説明書
- サードパーティ ライセンスなどの資料

その他の必要な装備

WebShield e500アプライアンスを19インチ ラックに組み込むにはマウンティング キットが必要です。また、ラック以外の場所に設置するには、適切に場所を確保し、アプライアンスを保護するための装備が必要となります。安全のための注意事項に常に従ってください。詳細については、3 ページの「電源および安全に関する情報」を参照してください。

アプライアンスの設定と管理を行うには、アプライアンスと同じネットワークに接続しているコンピュータ、またはアプライアンスに直接接続しているコンピュータが必要です。詳細については、32 ページの手順 4 を参照してください。これにより、コンピュータの Web ブラウザからアプライアンスのユーザ インターフェースにアクセスが可能になります。

設定用コンピュータの要件

アプライアンスのユーザ インターフェースは、Microsoft Internet Explorer バージョン 5.5 と 6.0 用に最適化されています。これ以外のバージョンまたは NetscapeNavigator には対応していません。

アプライアンスにアクセスすると、Web ブラウザに適切なコンポーネントがインストールされているかどうかチェックされます。不足しているコンポーネントがあれば、ダイアログボックスが表示されます。

Web ブラウザで次の機能を有効にしてください。

- Secure Sockets Layer（SSL）v3.0 暗号化
- JavaScript
- ActiveX（Microsoft Internet Explorer）
- プラグイン（Netscape Navigator）

以下の画面設定を使用すると、ユーザ インターフェースの表示が最適になります。

- 65,536 色（256 色以上）
- 1152x864 の解像度

ソフトウェアの復元とアップグレード

アプライアンスの一般的な管理作業以外に、次のような作業も必要になります。

- 予想外の問題が発生した場合に、アプライアンスの両ドライブにソフトウェアを復元する
- WebShield e500 アプライアンス アップグレード CD を使用し、アプライアンスのソフトウェアをアップグレードする

これらの作業を行うには、アプライアンスにキーボードとモニターを接続する必要があります。詳細については、61 ページを参照してください。

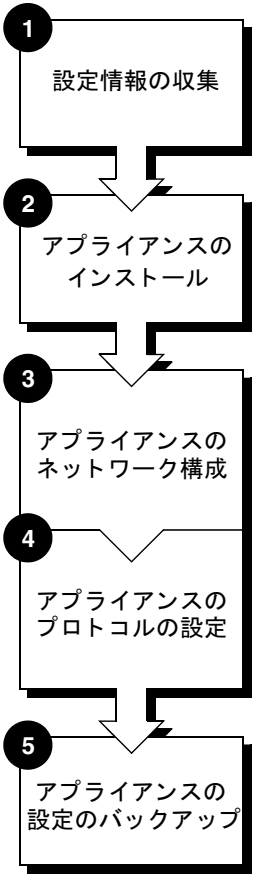
アプライアンスのウイルス定義ファイル（.DAT ファイル）とスキャン エンジンのアップデート

アプライアンスの自動アップデート機能により、.DAT ファイルとスキャン エンジンは常に最新の状態に保たれ、万全のウイルス対策保護が維持されます。この機能は、ユーザ インターフェース（Web ブラウザ）で設定することができます。詳細については、50 ページを参照してください。同じユーザ インターフェース画面からいつでもアップデートを開始することができます。

サービスパックと HotFix のインストール

サポート担当者から、アプライアンスのソフトウェアを強化するサービスパックや HotFix が提供されることがあります。これらは、ユーザ インターフェース（Web ブラウザを使用）からインストールすることができます。インストールに関する情報については、サービスパックまたは HotFix に付属の資料を参照してください。

アプライアンスの準備



アプライアンスの使用方法が決まったら（『製品ガイド』の第 1 章を参照）、次の作業を行い、WebShield アプライアンスをネットワークに統合します。

1. 必要な設定情報を収集します（19 ページを参照）。
2. 必要な場所にアプライアンスを設置し、適切に接続します（31 ページを参照）。
3. ネットワークの設定を行います（35 ページを参照）。
4. プロトコルの設定を行います（43 ページを参照）。
5. アプライアンスのソフトウェアを復元したときに、すばやく再設定を実行できるように、アプライアンスの設定情報をバックアップします（59 ページを参照）。

アプライアンスのインストールと設定を完了したら、ユーザ インターフェースにアクセスし、必要な機能を設定します。ユーザ インターフェースで機能を設定する方法については、ヘルプ ボタン（?）をクリックし、ヘルプ トピックを参照してください（57 ページを参照）。

インストールに必要なスキル

電子メール システムやインターネット ゲートウェイのインストールとアプライアンスの構成は、IT 管理者が行ってください。設定のプロセスでは、スキャン対象となるプロトコルに関する知識が必要となります。また、正しく設定しなければなりません。さらに、使用するモード（プロキシ モードまたは透過モード）に応じて、トラフィックがアプライアンスにルーティングされるように他の装置を構成しなければなりません。

詳細については、19 ページを参照してください。

ポートとコネクタ

vii ページに、アプライアンスのポートとコネクタを示します。ポートに機器を接続する方法については、31 ページのインストール手順を参照してください。

> **注意：**アプライアンスの外観は製造時に変更される可能性があります。したがって、アプライアンスのポートとコネクタの位置とタイプが、このガイドの説明と異なる場合があります。相違がある場合には、製品に付属のリリース ノートで最新の情報を確認してください。

以下では、これらのポートとコネクタについて説明します。

A 2 機のハードディスクドライブ

ドライブは両方ともホット接続が可能な RAID 1（ミラー）仕様の 17.4GB SCSI ハードディスク ドライブです。片方のドライブで予想外の問題が発生しても（ドライブ上の赤色の LED で通知）、シームレスな処理を行い、アプライアンスのオペレーティング システムとデータの処理をミラーリングします。ドライブはキャディに収められているため、アプライアンスの稼動中でも欠陥のあるドライブを交換することができます。交換したドライブのディスク イメージは、既存のドライブから自動的に作成されます。66 ページの「片方のハードディスクドライブ LED が赤く点灯している」を参照してください。

B CD-ROM ドライブ

CD-ROM ドライブはアプライアンスのソフトウェアを復元したり、アップグレードするときに使用します。他の用途には使用しないでください。詳細については、62 ページの手順 4 を参照してください。

C コントロール パネル

アプライアンスの右下にあるコントロール パネルには、システムの情報を提供する LED があります。リセット ボタンと電源ボタンもあります。

リセット ボタン
電源のオンとオフをシミュレートし、アプライアンスを再起動します。

電源ボタン
アプライアンスの電源をオンにします（電源 LED が点灯します）。電源ボタンがオフの場合、アプライアンスはスタバイ モードになっています。

アプライアンスがスタンバイ モードのとき、ネットワーク ポートはアクティブのままですが、アプライアンスへのプロトコルまたはデータは通過できません。これにより、組織のウイルス対策保護を維持します。

> **注意：**電源スイッチ E（アプライアンスの背面）がオフの場合、アプライアンスに電源が供給されません。

オーバーヒート LED
アプライアンスがオーバーヒートしたときに点灯します。オーバーヒートはユニットの周りで空気の流れが悪かったり、室温が正常に稼動できる状態を超えたときに起こります。ユニットの中央にある製品のファンのノイズを聞いて、ファンが動作しているかどうか確認してください。作していないと思われたら、アプライアンスの電源をオフにして、ご購入先までご連絡ください。

ネットワーク アクティビティ LED
ネットワーク ポートにネットワーク アクティビティが存在するとき（NIC 1 が LAN1 ポート、NIC 2 が LAN2 ポート）に点灯します。LED がオフのときにこの LED が点灯する場合、アプライアンスはスタンバイ モードになっています。

CD-ROM ドライブ アクティビティ LED
アプライアンスが CD-ROM ドライブの CD にアクセスしているときに点灯します。

電源 LED
アプライアンスの電源がオンになり、稼動状態になると点灯します。

D 電源ソケット

同梱されている電源コードを使用してアプライアンスをコンセントに接続します。

> **重要：**国で定められた規格に準拠している電源コードを使用してください。コードが適合していない場合はご購入先までお問い合わせください。

E 電源スイッチ

電源スイッチをオンにすると、アプライアンスに電源が供給されます。

> **注意：**電源スイッチ C がオンで、アプライアンスの前面にあるコントロール パネルの電源ボタンがオフの場合、アプライアンスはスタンバイモードになっています。

F キーボード ポート

アプライアンスのソフトウェアを復元したり、アップグレードしたりする場合にのみ、キーボードをこのポート（紫色）に接続します（62 ページの手順 1 を参照）。

G モニター ポート

アプライアンスのソフトウェアを復元したり、アップグレードしたりする場合にのみ、モニターをこのポートに接続します（62 ページの手順 2 を参照）。

H LAN1 ポート（NIC 1）

LAN1 ポートは RJ-45 10/100Mbps の自動検知式 Ethernet ネットワーク ポートです。アプライアンスを既存のネットワークに接続する場合に使用します（32 ページの手順 4 を参照）。

LAN1 ポートは次のトラフィックを送受信します。

- 送受信プロトコルのトラフィック
- 管理データとログ データ。アプライアンスのユーザ インターフェースへのアクセスに使用するリモート Web ブラウザからの接続も含まれます。アプライアンスで ePolicy Orchestrator を使用している場合には、ePolicy Orchestrator との通信もこのポート経由で送信されます。

LAN1 ポートのデフォルトの IP アドレスは 10.1.1.108（サブネット マスクは 255.255.255.0）で、初期状態では、このアドレスでアプライアンスにアクセスすることができます。アプライアンスを設定するときに、次の設定を行うことができます。

- ネットワークに有効な IP アドレスを追加します。
- デフォルトの IP アドレスを変更するか、無効にします。
- デフォルトの IP アドレスを削除し、使用されないようにします。

注意：以前のバージョンのアプライアンスでは、LAN1 ポートはデータ ポートと呼ばれていました。このバージョンからは、LAN1 ポートとなります。

---

❶ LAN2 ポート（NIC 2）

LAN2 ポートは RJ-45 10/100Mbps の自動検知式 Ethernet ネットワーク ポートで、その機能はアプライアンスの使用方法によって異なります。

- **プロキシ モード** ー LAN2 ポートはローカル管理接続にのみ使用されます。送受信プロトコル トラフィックの送受信には使用できません。

  このポートは、LAN1 ポートでリモート管理接続ができない場合に使用します。リモート管理接続ができない原因として、次の場合が考えられます。

  – LAN1 ポートの IP アドレスがリモート コンピュータとは別のサブネットに属している場合。

  – LAN1 ポートに設定した IP アドレスを忘れてしまった場合、またポートのデフォルト IP アドレス（10.1.1.108）が無効になっている場合。

- **透過モード** ー LAN2 ポートは LAN1 ポートと同様に、アプライアンスを既存のネットワークに接続します。LAN1 ポートと同じ種類のトラフィックの送受信を行います。

接続に関する情報については、32 ページの手順 4 を参照してください。

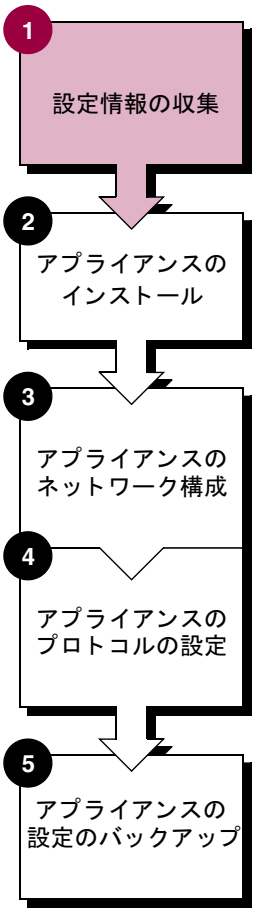
LAN2 ポートのデフォルトの IP アドレスは 10.1.2.108（サブネット マスクは 255.255.255.0）です。アプライアンスを設定するときに、次の設定を行うことができます。

- ネットワークに有効な IP アドレスを追加します。
- デフォルトの IP アドレスを変更するか、無効にします。
- デフォルトの IP アドレスを削除し、使用されないようにします。
- ポートを無効にし、使用されないようにします。

重要：透過モードを使用する場合、LAN2 ポートを無効にしないでください。

以前のバージョンのアプライアンスでは、LAN2 ポートは管理ポートと呼ばれていました。このバージョンからは、LAN2 ポートとなります。

設定情報の収集



アプライアンスの使用方法が決まったら（『製品ガイド』の第 1 章を参照）、必要な設定情報を収集する準備が整いました（手順 1）。

ここでは、収集が必要な情報について説明します。アプライアンスを短時間でセットアップできるように、インストールと設定を行う前に情報を収集しておいてください。

このガイドでは情報の記入欄が用意されています。

設定する情報とアプライアンスの動作については、『製品ガイド』の第 11 章を参照してください。

31 ページの手順 2、「アプライアンスのインストール」を参照してください。

アプライアンスのホスト名

アプライアンスに固有のホスト名を指定します。

ホスト名	

ドメイン

アプライアンスが参加しているドメインまたはサブドメインの完全修飾名を指定します。

ドメイン名	

例 :`myorg.com`, `network1.myorg.com`

ネットワーク アドレス

アプライアンスの TCP/IP ネットワーク アドレスを指定します。

	TCP/IP アドレス
LAN1 ポートの IP アドレスとサブネット マスク	. . . . . .
LAN2 ポートの IP アドレスとサブネット マスク	. . . . . .

ローカル DNS サーバの IP アドレス	. . .
デフォルト ゲートウェイまたはルータの IP アドレス	. . .

☐ **注意 :** LAN1 ポートと LAN2 ポートには、複数の IP アドレスを設定することができます。

以前のバージョンの WebShield アプライアンスでは、LAN1 ポートはデータ ポート、LAN2 ポートは管理 ポート呼ばれていました。このバージョンからはそれぞれ LAN1 ポート、LAN2 ポートとなります。

内部ネットワーク

アプライアンスが接続している内部ネットワーク（社内のネットワーク）のドメインまたは IP アドレスを指定します。必要な数の内部ネットワークが指定できます（以下には 10 ネットワーク分の記入欄があります）。

☐ **注意 :** ドメインを外部ネットワークとして扱う必要がない限り、アプライアンスが配置されているドメインを必ず指定してください。

ネットワーク	ドメイン、IP アドレス、サブネット マスク
例 1	myorg.com
例 2	192 . 168 . 1 . 0 255 . 255 . 255 . 0
例 3	*.myorg.com
1	. . . . . .
2	. . . . . .
3	. . . . . .
4	. . .

	.	.	.
5	.	.	.
	.	.	.
6	.	.	.
	.	.	.
7	.	.	.
	.	.	.
8	.	.	.
	.	.	.
9	.	.	.
	.	.	.
10	.	.	.
	.	.	.

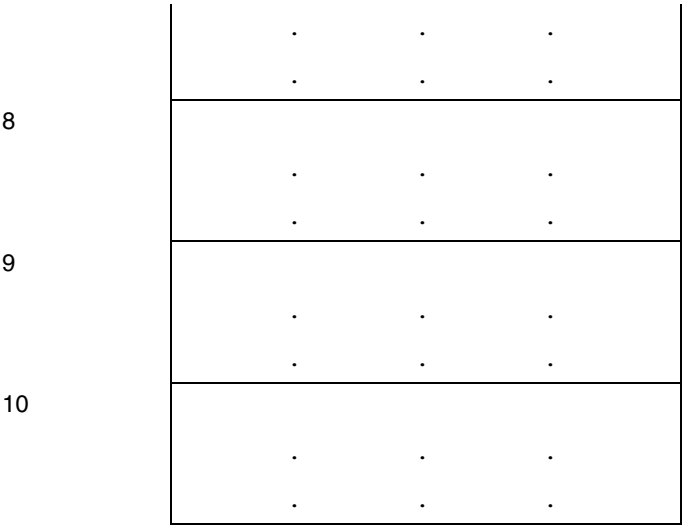
外部ネットワーク

アプライアンスが接続している外部ネットワーク（社外のネットワーク）のドメインまたは IP アドレスを指定します。必要な数のネットワークが指定できます（以下には 10 ネットワーク分の記入欄があります）。

重要 : アプライアンスがインターネット トラフィックのプロキシとして機能できるように、外部ネットワークには * ドメインを使用してください。

ファイアウォールの IP アドレスが含まれているか確認してください。

ネットワーク	ドメイン、IP アドレス、サブネット マスク
例 1	testing.myorg.com
例 2	sales.myorg.com
例 3	*
1	. . . . . .
2	. . . . . .
3	. . . . . .
4	. . . . . .
5	. . . . . .
6	. . . . . .
7	



プロキシ モードと透過モード

どのモードを使用するかを決定してください。使用できるモードはどちらか 1 つのみです。

☐ プロキシ モード（明示プロキシ）

☐ 透過モード（透過プロキシ）

2 つのモードの詳細については、『製品ガイド』の「プロキシ モードと透過モード」を参照してください。

重要 :2 つのモードはそれぞれ別のものです。アプライアンスのインストールと設定を行う前に、使用するモードをよく理解したうえで選択してください。

ネットワークを正しく動作させるために、アプライアンスの設定は正しい情報を元に行ってください。必要な情報についてご不明な点がある場合には、社内のネットワーク担当者にご相談ください。

静的ルーティングと動的ルーティング

ネットワークにアプライアンスを追加した場合は、ネットワーク全体がアプライアンスを経由して内部や外部と通信できるかどうかを確認する必要があります。アプライアンスで静的ルーティングや動的ルーティングを使用して、この情報を設定することができます。これにより、アプライアンスはネットワークのさまざまな部分にアクセスできます。

- **プロキシモード** ― アプライアンスがネットワーク全体と通信を行うために、複数のゲートウェイやルータを使用しなければならない場合があります。追加のゲートウェイやルータは静的ルーティングで設定してください。
- **透過モード** ― アプライアンス経由で行う内部や外部との通信の一部には、ルーティング情報を指定する必要がある場合もあります。このルーティング情報は、静的ルーティングとして指定してください。また、アプライアンスは RIP (Routing Information Protocol) と OSPF (Open Shortest Path First) のルーティング プロトコルをサポートしています。そのためネットワークがこのプロトコルを使用している場合には、動的ルーティングを使用してネットワークからルーティング情報を集めることができます。

それぞれの静的ルーティングには、ネットワークを区別するために IP アドレスとサブネット マスクを指定してください。また、ネットワークにアクセスするためのゲートウェイやルータにも IP アドレスを設定してください。必要な数の静的ルーティングを指定できます（以下には 4 ネットワーク分の記入欄があります）。

ルーティング	ネットワークの IP アドレスとサブネット マスク		ゲートウェイまたはルータの IP アドレス
例	192 . 168 . 40 . 0 255 . 255 . 255 . 0	→	192 . 168 . 50 . 3
1	. . . . . .	→	. . .
2	. . . . . .	→	. . .
3	. . . . . .	→	. . .
4	. . . . . .	→	. . .

動的ルーティングを使用してネットワークからルーティング情報を取得するには、次のチェックボックスをオンにします。

☐ 動的ルーティングの有効化

プロトコル

有効にするプロキシのチェックボックスと、強制的に実行するウイルス スキャンのチェックボックスをオンにします。プロトコル トラフィックを転送するポートがデフォルト（括弧内の値）と異なる場合には、そのポートを指定します。

	プロキシの有効化	受信トラフィックのスキャン	送信トラフィックのスキャン	ポート
E メール（SMTP）	☐	☐	☐	(25)
ファイル転送（FTP）	☐	☐	☐	(21)
Web ブラウズ（HTTP）	☐	☐	☐	(80)
メール ダウンロード（POP3）	☐	☐		(110)

☐ **注意：**アプライアンスは、方向（受信または送信）を区別せずにメール ダウンロード（POP3）トラフィックをスキャンします（29 ページの「メール ダウンロード（POP3）」を参照）。この理由から、チェックボックスは 1 つしか設けてありません。

スキャン プロファイル

以下のいずれかのボックスをチェックして、使用量プロファイルを選択します。

- ☐ 大量の SMTP、ある程度の HTTP、および最小限の FTP リソースを割り当てる
- ☐ 一定の SMTP、一定の HTTP、および最小限の FTP リソースを割り当てる
- ☐ 可変量の SMTP、一定の HTTP、および最小限の FTP リソースを割り当てる
- ☐ ユーザ指定値 - アプライアンスは、プロトコル設定のページ（ユーザ インターフェース）内の関連する設定値を使用して、必要な設定について設定値の指定を可能にしています。

注意：メールのダウンロード（POP3）プロトコルについては、使用量プロファイル内に設定を設けていません。このプロトコルは一般に、他のプロトコルに比べて使用頻度が低いからです。ただし、このプロトコルは他のプロキシと同様に、プロトコル設定ごとの正確な設定値は、プロトコル設定ページ（ユーザ インターフェース）で変更できます。必要に応じて、さらに調整を加えることも可能です。

以降のセクションでは、26 ページの「E メール（SMTP）」、28 ページの「ファイル転送（FTP）」、29 ページの「メール ダウンロード（POP3）」など、各種プロトコルのセットアップに必要なその他の情報について説明しています。

E メール（SMTP）

必要な配信方法のボックスをチェックします。

- ☐ ローカル ドメイン（以下を参照）
- ☐ DNS

  TCP/IP ネットワーク情報を入力したときに指定した DNS サーバが使用されます（19 ページの「ネットワーク アドレス」を参照）。

- ☐ 代替中継（28 ページを参照）

ローカル ドメイン

メール リレーについて以下の情報を指定します。必要な数のリレーが指定できます（以下には 15 ネットワーク分の記入欄があります）。最も一般的な中継を優先的に指定し、アプライアンスでその順番で中継されるようにしてください。

リレー	電子メール ドメイン		完全修飾ホスト名（メール サーバ）
例 1	*myorg.com*	➡	*mail.uk.myorg.com*
例 2	*myorg.co.uk*	➡	*mail1.us.myorg.com　mail2.us.myorg.com*
例 3	**.myorg2.com*	➡	*mail2.us.myorg.com*

1		➡	
2		➡	
3		➡	
4		➡	
5		➡	
6		➡	
7		➡	
8		➡	
9		➡	
10		➡	
11		➡	
12		➡	
13		➡	
14		➡	
15		➡	

代替中継

代替中継について以下の情報を指定します。必要な数のリレーが指定できます（以下には 15 ネットワーク分の記入欄があります）。最も一般的な中継を優先的に指定し、アプライアンスでその順番で中継されるようにしてください。

リレー	電子メール ドメイン		完全修飾ホスト名
例 1	*myorg.org*	→	*mail.externalorg1.com mail.externalorg2.com*
例 2	*	→	*outmail.myorg.com*
1		→	
2		→	
3		→	
4		→	
5		→	
6		→	
7		→	
8		→	
9		→	
10		→	
11		→	
12		→	
13		→	
14		→	
15		→	

ファイル転送（FTP）

FTP で 8 ビットの ASCII 転送をブロックするには、次のボックスをチェックします。

☐ ASCII モードでの 8 ビット データ転送をブロックする

注意 ：ファイル転送ユーティリティの中には、デフォルトで 8 ビット ASCII モードが使用されるものがあります。アプライアンスが 8 ビット ASCII モードをブロックする場合には、転送ユーティリティをバイナリ モードに変更してください。

FTP の詳細については、『製品ガイド』を参照してください。

メール ダウンロード（POP3）

汎用プロキシ

アプライアンスを経由して汎用プロキシ接続が確立されると、次のように、ユーザ名、ホスト名、ポート番号が # 記号とコロン（:）で区切られます。

```
user#host:port
```

別の区切り文字を使用する場合には、ここに指定してください。

ユーザ ☐ ホスト ☐ ポート

注意：汎用接続用のポートをアプライアンスに割り当てると、アプライアンス経由で汎用 POP3 接続を行うたびに、POP3 クライアント（ソフトウェア）でポート番号を指定する必要がなくなります。

専用プロキシ

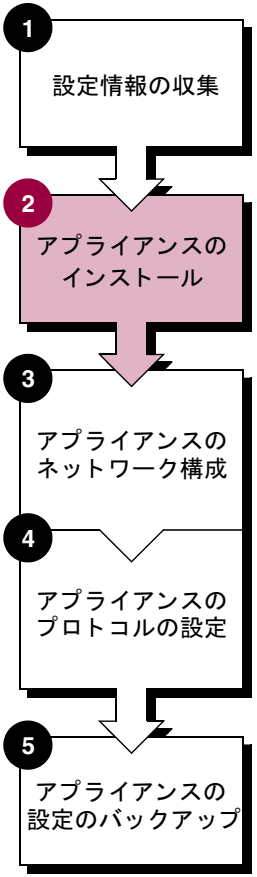
アプライアンスを経由して専用プロキシ接続が確立されると、POP3 サーバへのアクセスに特定のポートが使用されます。

必要な数のサーバ接続が指定できます（以下には 10 サーバ分の記入欄があります）。サーバごとに固有のポート番号とドメイン名を指定してください。

サーバ	ポート	POP3 サーバ ドメイン名
例	*1024*	*pop3server.externalorg.com*
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

POP3 の詳細については、『製品ガイド』を参照してください。

アプライアンスのインストール



構成に必要な情報を収集したら（19 ページを参照）、次に、アプライアンスを設置して接続します（手順 2）。

この章では、アプライアンスのインストール手順について説明します。操作を行う前にこの章をよく読み、作業内容を確認してください。

詳細については、10 ページを参照してください。

ネットワーク構成の設定については、35 ページの手順 3 を参照してください。

ポートとコネクタの詳細については、14 ページを参照してください。

WebShield e500 アプライアンスをインストールするには

1. 3 ページの「電源および安全に関する情報」で安全上の注意事項をよく読んで、指示に従ってください。
2. WebShield e500 アプライアンスをパッケージから取り出して、平らな場所に設置します。
3. 19 インチ ラックなどにアプライアンスを設置する場合には、安全上の注意事項に従ってアプライアンスを設置してください。3 ページの「電源および安全に関する情報」を参照してください。

    a. 設置場所を準備します。

    WebShield e500 アプライアンスを 19 インチ ラックに組み込むにはマウンティング キットが必要です。viii ページの指示に従ってください。

    アプライアンスを設置する場合は、換気が十分であることと、ポートにアクセス可能であることを確認してください。

    b. アプライアンスを設置します。

    アプライアンスが落下しないようにしっかり固定します。

4. 付属のネットワーク ケーブルを使用して、アプライアンスをネットワークに接続します。使用するポートとケーブルは、アプライアンスの使用方法によって異なります。

   - **プロキシ モード**

     LAN1 ポート ： 付属の青いネットワーク ケーブル（または同等の CAT 5 Ethernet ケーブル）を使用してアプライアンスの LAN1 ポート（17 ページの H を参照）を既存のネットワークに接続します（図 4-2）。ケーブルはストレート ケーブルです（クロスケーブルではありません）。そのため、ネットワーク機器にある通常のストレート（MDI）RJ-45 ポートにアプライアンスを接続できます。

     また、この接続により、リモート コンピュータからネットワーク経由でアプライアンスを管理することができます。

     LAN2 ポート ： プロキシ モードの場合、アプライアンスの LAN2 ポートは専用の管理ポートになります。アプライアンスをローカルで管理する場合は、付属のオレンジ色のネットワークケーブル（または同等の CAT 5 Ethernet クロスケーブル）を使用して、LAN2 ポート（18 ページの I を参照）とローカル コンピュータのネットワーク カードとを接続します（図 4-2 を参照）。

     アプライアンスをローカルで管理する場合は、この接続のみ設定する必要があります。

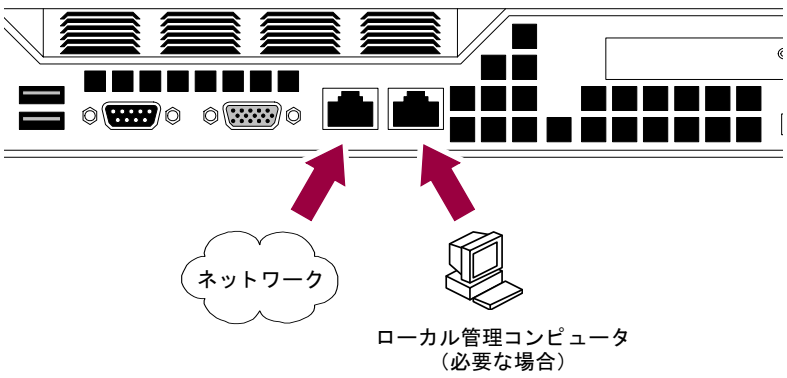


図 4-2. アプライアンスの接続 （プロキシ モード）

- **透過モード**

  LAN1 および LAN2 ポート：付属の青いネットワーク ケーブル（または同等の CAT 5 Ethernet ケーブル）を使用してアプライアンスの LAN1 ポート (17 ページの H を参照) と LAN2 ポート（18 ページの I を参照）を既存のネットワーク（図 4-3）に接続します。これによりアプライアンスがデータ ストリームに挿入されます。ケーブルはストレート ケーブルです（クロスケーブルではありません）。そのため、ネットワーク機器にある通常のストレート（MDI）RJ-45 ポートにアプライアンスを接続できます。

  注意：透過モードでは、アプライアンスは異なる 2 つのサブネットに接続していなければなりません。

  アプライアンスはファイア ウォールの内側で使用してください。例えば、ネットワークがハブとファイアウォールを通して接続されている場合、アプライアンスをハブとファイアウォールの間に設置し、ハブを LAN1 ポートに、ファイアウォールを LAN2 ポートに接続します。

  透過モードの場合、リモート コンピュータからネットワーク経由でアプライアンスを管理することができます。ただし、LAN2 ポートはトラフィックの送受信をするため、LAN2 ポートを通してローカル管理接続を取得（プロキシ モードでのみ可能な方法）することはできません。

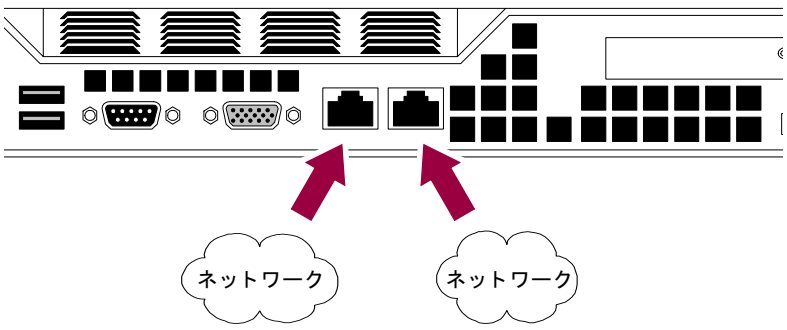


図 4-3. アプライアンスの接続 （プロキシ モード）

5. 付属の電源コードを使用して、アプライアンスの電源ソケット（16 ページの D を参照）とコンセントに接続します。

重要: 国で定められた規格に準拠している電源コードを使用してください。コードが適合していない場合はご購入先までお問い合わせください。

アプライアンスは、ソフトウェアがインストールされた状態で出荷されます。指示がない限りアプライアンスの CD-ROM ドライブに CD を挿入しないでください。

---

6. 電源スイッチと電源ボタンの両方をオンの位置にして、アプライアンスの電源をオンにします（図 4-4）。

   電源スイッチは装置の背面にあります（16 ページの E を参照）。電源ボタンは装置の前面のコントロール パネルにあります（15 ページの C を参照）。

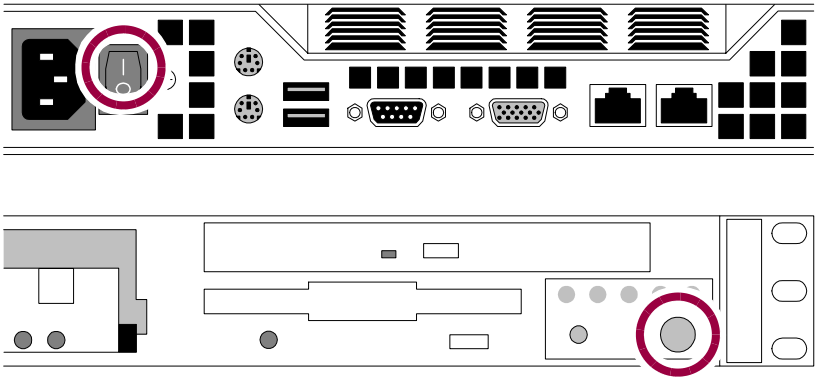
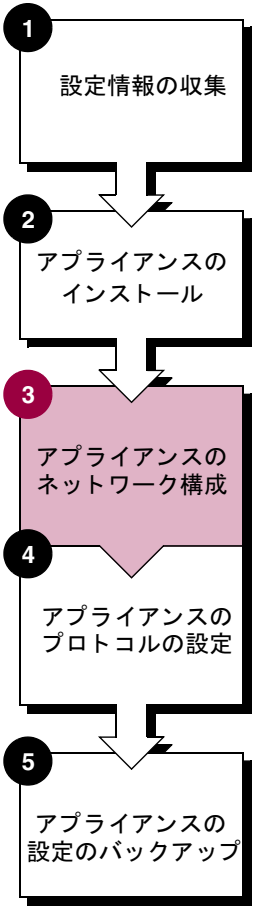


図 4-4. アプライアンスの電源投入

アプライアンスの電源をオンにすると、起動シーケンスが実行され、約 2 分で使用可能になります。次に、アプライアンスのネットワーク構成を設定します。35 ページに進んでください。

ネットワーク構成の設定



アプライアンスを所定の場所に設置し、必要な接続が完了したら（31 ページ）、次にネットワークの設定を行います（手順 3）。

ここでは、ネットワークの設定方法について説明します。操作を行う前にこの章をよく読み、作業内容を確認してください。

必要な設定情報の収集（19 ページ）が既に終わっている場合は、設定をよりすばやく進めることができます。

アプライアンスのソフトウェアを復元またはアップデートするには、61 ページを参照してください。

既に作成済みの設定ファイルを使用してアプライアンスの設定を復元するには、60 ページの「設定の復元」を参照してください。

プロトコルの設定については、43 ページの手順 4 を参照してください。

アプライアンスのデフォルトの設定については、『製品ガイド』の付録 A を参照してください。

アプライアンスのネットワーク構成を設定するには

1. アプライアンスを管理するコンピュータで Web ブラウザを開きます。
2. ［アドレス］フィールド（Web サイトを開くために URL を入力するところ）に、次のアドレスを入力します。

   `https://<IP address>`

> **注意：** `http` ではなく、`https` と入力してください。

使用する IP アドレスは、アプライアンスに接続する方法によって異なります。

- LAN1 ポートを通して、ネットワーク経由でアプライアンスにリモート接続している場合は、アプライアンスに設定した LAN1 ポートの IP アドレスを使用してください（デフォルトは `10.1.1.108` です）。

- LAN2　ポートを通して、ネットワーク経由でアプライアンスにリモート接続している場合（透過モードでのみ可能）、アプライアンスに設定した LAN2 ポートの IP アドレスを使用してください（デフォルトは `10.1.2.108` です）。
- ローカルで、LAN2 ポートに直接接続している場合（プロキシ モードでのみ可能）、アプライアンスに設定した LAN2 ポートの IP アドレスを使用してください（デフォルトは `10.1.2.108` です）。

注意：アプライアンスを透過モードで使用する場合は、管理コンピュータが接続されているポートとサブネットの IP アドレスを使用します。

管理用の接続では、常に Secure Sockets Layer（SSL）暗号化機能が使用されるので、安全に接続することができます。［**ログオフ**］をクリックして管理セッションを終了すると、SSL 接続は切断されます。長時間の管理セッションで安全性を維持するため、無通信時間が 15 分を超えた場合も SSL 接続は切断されます。

LAN1 ポートまたは LAN2 ポート (39 ページの手順 16 を参照) に新しい IP アドレスを設定すると、新しいアドレスが追加されます。デフォルトの IP アドレスは上書きされません。アプライアンスをプロキシ モードで使用する場合、LAN2 ポートの IP アドレスは別のアドレスで、LAN2 ポートにのみ使用され、LAN1 ポートから参照することはできません。このアドレスは無効にすることができます。LAN　1 ポートにアクセスできない場合に、LAN2 ポートに直接アクセスして、アプライアンスの管理を行うことができます。

管理コンピュータ（アプライアンスの管理用コンピュータ）の Web ブラウザで、アプライアンスが Web ブラウザのプロキシとして設定されていないか確認してください。設定されている場合は、管理接続できません。

さらに、管理コンピュータとアプライアンスの間にプロキシが存在する場合は、プロキシをアプライアンスのハンドオフ ホストとして設定しておく必要があります。

---

3. Web ブラウザがアプライアンスを検出すると、セキュリティ警告メッセージが表示され、セキュリティ証明書の受信が確認される場合があります。［**はい**］をクリックして、証明書を受信します。

> **ヒント：**セキュリティ警告メッセージは、ブラウザ セッションのたびに表示されます。このメッセージが表示されないようにするには、証明書を表示してインストールし、自動的に受け取るようにします。Internet Explorer の場合、セキュリティ警告メッセージで［**証明書の表示**］をクリックし、表示されたダイアログボックスで［**証明書のインストール**］をクリックします。

アプライアンスの電源を入れた直後は、起動シーケンスが終了するまで約 2 分待つ必要があります。そうしないと、Web ブラウザがアプライアンスを検出できない場合があります。その場合は、同じ URL に再度アクセスしてください。それでも［ログオン］ページにアクセスできない場合は、67 ページを参照してください。

アプライアンスの［ログオン］ページが表示されます。アプライアンスでは、そのインターフェースの実行に必要なコード サポートが Web ブラウザにインストールされているかどうかをチェックします。このため、セキュリティ警告やダウンロードのダイアログボックスが表示される場合があります。ダイアログボックスで必要な情報を入力してください。

> **注意：**アプライアンスのユーザ インターフェースを実行するには、Java 2 ランタイム環境が必要です。この環境を Web ブラウザにインストールする場合には、ブラウザで必要とするコンポーネントに応じて、5 ～ 14MB の空き容量が必要になります。また、速度の遅いリモート回線を使用している場合には、インストールにかかる時間が長くなります。

4. ［**言語**］でアプライアンスのインターフェースで使用される言語を選択します。

   選択した言語によってアプライアンスの動作が変わることはありません。詳細については、39 ページの手順 14 を参照してください。

5. 英語を使用する場合は、地域を選択します。これにより、インターフェースを使用する場合に英語ではない文字を使用することができます。

6. ［**ログオン**］をクリックします。

   ［ネットワーク パスワードの入力］ダイアログ ボックスが表示され、ユーザ名とパスワードの入力が要求されます。ユーザ名は e500 で、デフォルトのパスワードは e500changeme です。以前の設定を使用せずにアプライアンスのソフトウェアを復元すると、パスワードはデフォルトのパスワードに戻ります。

7. ユーザ名およびパスワードを入力し、［**OK**］をクリックします。

   アプライアンスのユーザ インターフェースが開き、［システム設定］ページが表示されます。

   アプライアンスの設定が済んでいる場合は、画面の左側にナビゲーション バー付きの［システム状態］ページが表示されます。［システム設定］ページを表示するには、ナビゲーション バーで［**システム設定**］を選択します。ユーザ インターフェースの詳細については、57 ページの「アプライアンスの使用方法」を参照してください。各ページでの設定方法については、ヘルプボタン（?）をクリックして、当該ページのヘルプトピックを参照してください。

   注意 : アプライアンスの以前のバージョンの設定ファイルがある場合は、設定復元パネルを使用してアプライアンスの設定を復元できます。60 ページの「設定の復元」を参照してください。

   ---

8. ［**アプライアンス名**］ボックスに、アプライアンスのホスト名を 15 文字以内で入力します（19 ページの「アプライアンスのホスト名」を参照）。固有の名前を入力してください。

9. ［**DNS サーバ**］ボックスに、ローカル DNS サーバの IP アドレスを入力します。

10. ［**ドメイン名**］ボックスに、アプライアンスが参加しているドメインまたはサブドメイン名（myorg.com など）を入力します（19 ページの「ドメイン」を参照）。

11. ［**DNS サーバ**］ボックスに、ローカル DNS サーバの IP アドレスを入力します（19 ページの「ネットワーク アドレス」を参照）。

12. ネットワークとの通信にデフォルトのゲートウェイまたはルータ（ファイアウォール）を経由する場合は、ゲートウェイまたはルータの IP アドレスを［**既定のゲートウェイ**］ボックスに入力します（19 ページの「ネットワーク アドレス」を参照）。

    アプライアンスがネットワーク全体と通信を行うために、複数のゲートウェイやルータを使用しなければならない場合があります。その場合は、追加のゲートウェイとルータを静的ルーティングとして指定できます。41 ページの手順 22 を参照してください。

13. アプライアンスを透過モードで使用するには、[**透過モードの有効化**] を選択してください。アプライアンスをプロキシ モードで使用する場合は、このチェックボックスをチェックしないでください（23 ページの「プロキシ モードと透過モード」を参照）。

14. [**システム言語**] で、アプライアンスで使用する言語を選択します。

    ここで選択した言語は、アプライアンスで生成されたレポートやメッセージに適用されます。ただし、インターフェースから指定または修正できる文字列には適用されません。また、この言語設定は、アプライアンスにログオンしたときに選択したインターフェース表示用の言語の設定とは異なります（37 ページの手順 4 を参照）。

15. LAN の IP アドレスパネルが表示されない場合、[**LAN の IP アドレス**] をクリックしてパネルを表示します。

    このパネルでは、LAN1 ポートと LAN2 ポートに設定された IP アドレスのリストを表示します。

16. LAN1 と LAN2 のリスト下部の [**追加**] ボタンを使用して、LAN ポートへの新しい IP アドレスを指定してください（19 ページの「ネットワーク アドレス」を参照）。

    各ポートに複数の IP アドレスを指定することができます。変更を適用すると (42 ページの手順 27 を参照)、各ポートに新しい IP アドレスが追加されます。新しい IP アドレスを追加しても、既存の IP アドレスは上書きされません。不要な IP アドレスがある場合は次のいずれかの手順に従ってください。

    - IP アドレスを変更または無効にするには、該当 IP アドレスをリストで選択し、[**変更**] をクリックします。無効にする場合は、[**ネットワークアドレスを無効にする**] を選択します。
    - 削除する場合は、該当 IP アドレスをリストで選択し、[**削除**] をクリックします。

    > **注意：**新しい IP アドレスが機能するか確認するため、初期設定が完了したら、デフォルトの IP アドレスを削除する前に、新しいアドレスでアプライアンスにアクセスしてください。

    アプライアンスをプロキシ モードで使用する場合、LAN2 ポートは専用の管理ポートになり、直接的なローカル管理接続ができます。

17. アプライアンスへの直接管理接続を防ぐには、LAN2 ポートを無効にします。LAN2 リストの下部の［**無効**］を選択してください。

重要：透過モードを使用する場合は、LAN2 ポートを無効にしないでください。

アプライアンスを通過するトラフィックのソースが内部か外部かを判別するため、2 つのリスト（［内部ネットワーク］と［外部ネットワーク］）が使用されます。

ヒント：testing.myorg.com など、内部ネットワークに外部ネットワークとして扱いたいサブドメインがある場合には、［内部ネットワーク］と［外部ネットワーク］リストを次のように使用します。

内部ネットワーク：

```
*.myorg.com
```

外部ネットワーク：

```
testing.myorg.com
*
```

---

18. ［**内部ネットワーク**］をクリックし、［内部ネットワーク］パネルを表示します。

19. このパネルを使用して、保護対象とする組織内（ファイアウォールの内側）の内部ネットワークのドメインまたは IP サブネットを指定します（20 ページの「内部ネットワーク」を参照）。必要な数のネットワークが指定できます。

注意：アプライアンスが参加しているドメイン（38 ページの手順 10 で指定）を保護対象にするには、このドメインを内部ネットワーク リストに追加する必要があります。

ネットワークを追加するには、［**追加**］をクリックし、表示された［追加］ダイアログボックスで、ドメインまたは IP アドレスとサブネットマスクを指定します。［**OK**］をクリックして、ネットワークを内部ネットワーク リストに追加します。

20. ［**外部ネットワーク**］をクリックし、［外部ネットワーク］パネルを表示します。

    このパネルでは、アプライアンスにとって外部として設定されたネットワークを表示します。デフォルトでは、内部ネットワークで指定された以外のすべてのネットワークが外部ネットワークとして識別されるため、外部ネットワーク リストでは * がワイルドカードとして使用されます。

    重要：アプライアンスがインターネット トラフィックのプロキシとして機能できるように、外部ネットワークには * ドメインを使用してください。

    ファイアウォールの IP アドレスが含まれているか確認してください。

    ---

21. このパネルを使用して組織外 (ファイアウォールの外側) の外部ネットワークのドメインまたはIPサブネットを指定します。必要な数のネットワークが指定できます（22 ページの「外部ネットワーク」を参照）。

    ネットワークを追加するには、［**追加**］をクリックし、表示された［追加］ダイアログボックスで、ドメインまたは IP アドレスとサブネットマスクを指定します。［**OK**］をクリックして、ネットワークを外部ネットワーク リストに追加します。

22. アプライアンスとネットワークのさまざまな部分とが通信を行うために静的ルーティングを設定する必要がある場合は（24 ページの「静的ルーティングと動的ルーティング」を参照）、［**静的ルーティング**］をクリックして［静的ルーティング］パネルでルーティングを指定します。

23. 透過モードで動的ルーティングを使用したい場合は、［**動的ルーティング**］をクリックして［**動的ルーティングを有効にする**］を選択します。

    動的ルーティングは、ネットワーク上のルータが発信するルーティング情報を、アプライアンスを含めたネットワーク機器がリスンするようにするシステムです。アプライアンスがサポートするルーティング プロトコルは RIP (Routing Information Protocol) と OSPF (Open Shortest Path First) のみです。

24. ［**時刻とパスワードの設定**］をクリックして、［時刻とパスワードの設定］パネルを表示します。

25. 現在の日付と時刻を反映するように、[**時間帯**]、[**日付**]、および [**時刻**] の値を変更し、[**今すぐ設定**]をクリックします。時刻は 24 時間形式です。

    アプライアンスの日付と時刻が変更されます。これらの値は、トラフィックがアプライアンスを通過するときのタイムスタンプや、ログと警告の生成時に使用されます。

26. パスワードを変更するには、新しいパスワードを [**パスワード**] ボックスに入力し、[**確認**] ボックスに再度入力します。[**今すぐ設定**] をクリックします。

    > **重要 :** 安全性の観点から、アプライアンスに最初の設定をする際にデフォルトのパスワードを変更するようにしてください。

27. [**全ての変更を適用**] をクリックします。

    Web ブラウザからアプライアンスに変更が送信されます。IP の設定を変更したため、ソフトウェアの再起動を要求するメッセージが表示されます。

28. [**今すぐ再開**] をクリックします。

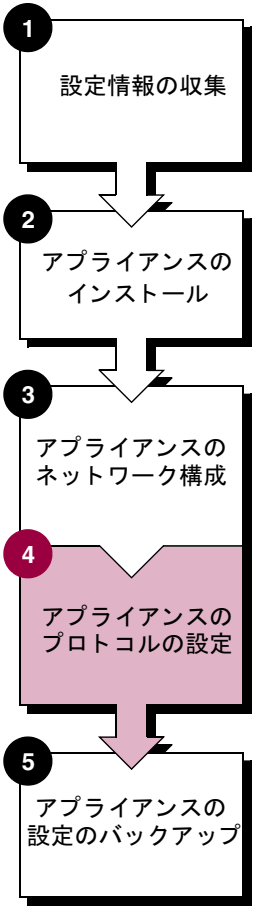
    アプライアンスが再起動し、約 2 分後に使用可能になります。

    新しい IP アドレスでユーザ インターフェースにアクセスできるように、新しい URL のホットリンクが表示されます。

29. アプライアンスが再起動したら、URL ホットリンクをクリックするか、管理用ポートに設定した IP アドレスの 1 つを入力します。LAN2 ポートを使用していたが、LAN2 ポートの IP アドレスを無効にした場合 (40 ページの手順 17) は、ネットワーク経由で LAN1 ポートにアクセスしてください。

    ログオンすると、画面の左側にナビゲーション バー付きの [システム状態] ページが表示されます。次に、アプライアンスのプロトコルを設定します。43 ページの「プロトコルの設定」に進んでください。

プロトコルの設定



ネットワークの設定（35 ページを参照）が終了したので、次にプロトコルの設定を行います（手順 4）。

ここでは、プロトコルの設定方法について説明します。操作を行う前にこの章をよく読み、作業内容を確認してください。

必要な設定情報の収集（19 ページ）が既に終わっている場合は、設定をよりすばやく進めることができます。

設定のバックアップについては、59 ページの手順 5 を参照してください。

作業

ここでは、必要な操作をいくつかの作業に分けて説明します。以下の操作は順番どおり実行してください。

1. アプライアンスのプロトコルを設定します（44 ページを参照）。
2. ウイルス定義（.DAT）ファイルとスキャン エンジンをアップデートし、完全なウイルス対策機能を維持するために、自動アップデート機能を設定します（50 ページを参照）。
3. 必要であれば、アプライアンスを経由してプロトコル トラフィックをルーティングするために、ファイアウォール、メール サーバ、Web キャッシュなどの装置を設定します。51 ページを参照してください。
4. 送受信トラフィックをスキャンし、ウイルス感染が正しく検知できるかどうか、設定をテストします（53 ページを参照）。

プロトコルの設定

WebShield e500 アプライアンスは、SMTP、FTP、HTTP、および POP3 の各プロトコルのプロキシを装備しています。アプライアンスのリソースはプロキシ間で分割されています。デフォルトでは、各プロトコルの送受信トラフィックをスキャンします（POP3 のトラフィックは方向を区別しません）。プロキシとプロトコルの詳細については、14 ページの「ポートとコネクタ」を参照してください。

有効とするプロトコル、ウイルス スキャンを実行するプロトコルの設定、および適切な使用率プロファイルを選択するには：

1. 特定のプロトコルのプロキシを無効にする（そのプロトコルのトラフィックがアプライアンスを通過しないように設定する）には、［システム設定］ページの［**有効なプロトコル**］セクションで、該当するプロトコルのチェックボックスの選択を解除します。

   注意：透過モードの場合、これによってアプライアンスを通過するトラフィックを防ぐことはありません。

2. 有効なプロトコルで受信または送信時のウイルス　スキャンを無効にするには、ナビゲーションバーで対応する［**設定**］のページ（［電子メールの設定］、［ファイル転送設定］、［Web 参照設定］、または［メールのダウンロード設定］）を選択し、［**受信トラフィックのスキャン**］または［**送信トラフィックのスキャン**］の選択を必要に応じて解除します（［**POP3 トラフィックのスキャン**］は［メールのダウンロード設定］ページで使用されます）。

   警告：ネットワークの別の場所でトラフィックをスキャンしている場合を除き、**有効になっているプロトコルのウイルス スキャンは無効にしないでください。**社内ネットワークを出入りするトラフィックのスキャンを無効にしている間は、ウイルスの感染を許すことになります。

   必要に応じて、他のネットワーク機器がアプライアンスを経由してプロトコルをルーティングするように設定されているかどうか、また、アプライアンスを迂回するものが存在しないかどうか確認します（51 ページを参照）。

3. ナビゲーション バーで、［**システム プロファイル**］を選択します。

4. 最も適切な使用量プロファイルを選択します（26 ページの「スキャン プロファイル」）。

   メール ダウンロード（POP3）プロトコルは、他のプロトコルより必要な帯域幅がはるかに少ないので、使用量プロファイルに含まれません。POP3 プロトコルのスキャンを有効にしている場合、選択したプロファイルにかかわらず、このプロトコルはスキャンされます。

   使用量の値（POP3 レベルを含む）は、いずれもプロトコルの［設定］ページで調整できます。値を調整すると、［システムプロファイル］ページで［**各プロトコルの「設定」ページで選択されている値を使用する** ］が自動的に選択されます。

5. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

プロトコルで使用されるポートの設定

各プロトコルで使用されるデフォルトのポートは次のとおりです。

- 電子メール（SMTP）: 25
- ファイル転送（FTP）: 21
- Web ブラウズ（HTTP）: 80
- メール ダウンロード（POP3）: 110

社内のネットワークでプロトコルごとに異なるポートを使用している場合には、それに合わせてアプライアンスのポート番号を調整する必要があります。

プロトコルに使用するポートを変更するには :

1. ナビゲーション バーで、プロトコルの［**設定**］ページを選択します。
2. ［**リスンポート**］ボックスに、必要なポート番号を入力します（25 ページの「プロトコル」を参照）。
3. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

電子メール（SMTP）の配信方法の設定

電子メール プロトコルが有効（デフォルトの設定）になっている場合には、使用する配信方法を設定する必要があります。

ここでは、アプライアンスがトラフィックのスキャンと配信を開始できるように、電子メールの配信方法に設定しなければならない情報についてのみ説明します。このプロトコルに関連するページは多数あります。これらのページでの設定方法について

は、ヘルプ ボタン (?) をクリックして該当するヘルプ トピックを表示してください (57 ページを参照)。

電子メール（SMTP）の配信方法を設定するには：

1. ナビゲーション バーで、[**電子メールの配信**] を選択します。
2. [使用する方法] パネルで配信方法を選択します（ 26 ページの「E メール（SMTP）」を参照)。
3. 配信方法として [**ローカル ドメイン**] を選択した場合には、[**ローカル ドメイン**] をクリックし、表示されたパネルでメール中継を指定します。必要な数のメール中継が指定できます（26 ページの「ローカル ドメイン」を参照)。

   メール転送は、特定のドメイン（myorg.com など）宛ての電子メール メッセージを、対応するメール サーバ（mail1.myorg.com など）にルーティングします。メール転送を追加するには、[**追加**] をクリックし、表示された [追加] ダイアログボックスで電子メール ドメインおよびホスト（メール サーバ）を指定します。[**OK**] をクリックして、ローカル ドメイン一覧に追加します。

ヒント：メール転送は一覧の順番に試行されます。ある転送がメッセージの条件を満たす場合、そのメッセージでは他の転送は試行されません。そのため、[**上へ**] および [**下へ**] ボタンを使用して、転送を必要な順序に並べてください。最も使用頻度の高い転送を一覧の一番上に配置します。

---

4. 配信方法として［**代替中継**］を選択した場合には、［**代替中継**］をクリックし、表示されたパネルでメール中継を指定します。必要な数の代替中継が指定できます（28 ページの「代替中継」を参照）。

   代替中継は、他の配信方法では配信できない電子メール メッセージをルーティングします。代替中継を追加するには、［**追加**］をクリックし、表示された［追加］ダイアログボックスで電子メール ドメインおよびホスト（メール サーバ）を指定します。［**OK**］をクリックして、代替中継一覧一覧に追加します。

   ヒント：ドメインにワイルドカード記号（*）を使用すれば、すべてのドメインからのメッセージをルーティングするメール中継を作成することができます。代替中継一覧で、他のエントリより下にワイルドカードを置くと、他のエントリが試行された後に、ワイルドカードが試行されます。

   代替中継一覧には、ローカル ホスト（メール サーバ）へ中継を含めることができます。これにより、DNS サーバ参照の後にローカル ドメインを試行することで、配信不能メッセージを組織にルーティングすることができます。

   メール転送は一覧の順番に試行されます。ある転送がメッセージの条件を満たす場合、そのメッセージでは他の転送は試行されません。そのため、［**上へ**］および［**下へ**］ボタンを使用して、転送を希望の順に並べてください。最も使用頻度の高い転送を一覧の一番上に配置します。

   ---

5. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

8 ビット データ転送を許可するかどうかの設定

ファイル転送プロトコル（FTP）は、コンピュータ間でのデータ転送を可能にするプロトコルです。このプロトコルは、バイナリと 8 ビット ASCII の 2 つのモードで動作します。バイナリ モードでは、異なるプラットフォーム間でも一定であるため、データを有効にスキャンすることができます。

注意：デフォルトでは、8 ビット ASCII 転送モードはブロックされます。これは、ASCII モードのデータにはさまざまな文字コードおよびファイル形式（使用するコンピュータシステムによる）が含まれるため、ウイルスが身を隠しやすくなるためです。

ファイル転送プロトコルが有効（デフォルトの設定）の場合、8 ビット データ転送を有効にすることができます。

8 ビット データ転送を有効にするには :

1. ナビゲーション バーで、［**ファイル転送設定**］を選択します。
2. ［**アスキーモードで 8 ビットデータ転送をブロックする**］の選択を解除します（28 ページの「ファイル転送（FTP）」を参照）。
3. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

> **注意 :** ファイル転送ユーティリティの中には、デフォルトで 8 ビット ASCII モードを使用するものがあります。ユーティリティのモードは必ずバイナリ モードに変更してください。

メール ダウンロード (POP3) プロキシの設定

メール ダウンロード プロトコルが有効（デフォルトの設定）の場合、区切り文字（汎用プロキシ接続用）とポート番号（専用プロキシ接続用）が設定できます。

WebShiled アプライアンスを経由して汎用プロキシ接続が確立されると、次のようにユーザ名、ホスト名、ポート番号が # 記号とコロン（:）で区切られます。

```
user#host:port
```

POP 汎用プロキシ接続の区切り文字を変更するには :

1. ナビゲーション バーで、［**メールのダウンロード設定**］を選択します。
2. 新しく使用する区切り文字を指定します（29 ページの「汎用プロキシ」を参照）。
3. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

POP3 専用プロキシ接続のポートを指定するには :

1. ［メールのダウンロード設定］ページで、専用プロキシ接続一覧にポート番号と POP3 サーバを指定します。指定できるサーバの個数は無制限ですが、対応するポート番号は一意である必要があります（30 ページの「専用プロキシ」を参照）。

   POP3 サーバを追加するには、［**追加**］をクリックし、表示された［追加］ダイアログボックスで一意のポート番号（一般に 1024 から 32767）とサーバのドメイン名（pop3server.externalorg.com など）を指定します。［**OK**］をクリックして、専用プロキシ接続一覧に追加します。
2. ［**全ての変更を適用**］をクリックします。

Web ブラウザからアプライアンスに変更が送信されます。

自動アップデートの設定

自動アップデート機能は、ウイルス定義（.DAT）ファイルおよびスキャン エンジンを更新し、完全なウイルス対策機能を維持するための機能です。

重要：設定に従ってウイルス スキャンが実行されるとき、ウイルスの検索と削除にはウイルス スキャン エンジンおよび現在の.DATファイルが使用されます。毎日新しいウイルスが多数発見されるため、McAfee 社ではウイルス対策用の定義ファイルを作成しています。さらに、ウイルス スキャン エンジンの新バージョンも作成しています。

自動アップデートを設定するには：

1. ナビゲーション バーで、［**ウイルス対策**］の［自動アップデート］を選択します。
2. ［FTP ダウンロードサイト］パネルで、.DAT ファイルとスキャン エンジンのコピー元を指定します。デフォルトでは、.DAT ファイルとスキャン エンジンは Network Associates の FTP サーバ（ftp.nai.com）から取得されます。

   別の FTP サーバを使用するには、次のテキストボックスの内容を変更します。

   - **サーバ名**
   - **.DAT/ エンジン ファイルのパス**
   - **サーバ ユーザ名**（オプション）
   - **パスワード**（オプション）

   接続するためにプロキシ サーバを経由する必要がある場合は、次のテキストボックスにサーバについての情報を入力してください。

   - **プロキシ サーバ**
   - **プロキシのポート番号**
   - **プロキシ ユーザ名**（オプション）
   - **プロキシのパスワード**（オプション）

   このページの設定に関する情報の詳細については、ヘルプボタン（?）をクリックして対応するヘルプトピックを表示してください。
3. ［**FTP アップデート スケジュール**］をクリックし、.DAT ファイルおよびスキャン エンジンを更新する日時（24 時間制）を選択します。
4. ［**全ての変更を適用**］をクリックします。

   Web ブラウザからアプライアンスに変更が送信されます。

他の機器の設定

ここでは、既存のネットワークにアプライアンスを完全に統合するために、他の機器に必要な変更について簡単に説明します。必要な変更は、アプライアンスをプロキシ モードまたは透過モードで使用しているかによって異なります。

- **プロキシ モード**（明示プロキシ）― プロトコルがアプライアンスを経由するようルーティングし、迂回するものがないように、他のネットワーク機器を設定する必要があります。アプライアンスをプロキシ サーバとして使用するすべての内部クライアント（HTTP、FTP、POP3 ソフトウェアなど）の設定も対象となります。特に、Web クライアントの HTTP、FTP、および Gopher の設定が HTTP ポート番号を使用するよう設定されているかどうか確認してください。下記の「アプライアンスを経由したプロトコルのルーティング」を参照してください。

- **透過モード**（透過プロキシ）― その名の通り、透過モードではネットワーク装置の再設定をほとんどすることなくアプライアンスをネットワークに組み込むことができます。しかし、電子メール トラフィックがアプライアンスを通過するように、SMTP 電子メールシステムの設定を行う必要があります。52 ページの「DNS サーバのレコードの変更」を参照してください。

重要：電子メールを毎日使用すると、メール サーバをオフラインにして設定を変更したり、メンテナンスを行う必要が生じる場合があります。その際、アプライアンスを起動したままメールを受信し、スキャンすることはできますが、転送することはできません。ただし、メール サーバにバックアップを作成するよう電子メールを設定している場合は例外となります。上限までメッセージを受信するようにアプライアンスを設定すると、容量不足になります。この問題を避けるには、メール サーバがオフラインのときは、アプライアンスの SMTP プロキシを無効にします。このようにすると、ファイアウォールが受信メッセージを配信不能として戻します。

アプライアンスを経由したプロトコルのルーティング

オプションの設定方法の詳細については、他の機器に付属するマニュアルを参照してください。機器の設定が完了したら、53 ページのテストを実行して、メールの設定が正しいかどうか確認することができます。各プロトコルで使用されるデフォルトのポートは次のとおりです。

- 電子メール（SMTP）: 25
- ファイル転送（FTP）: 21
- Web ブラウズ（HTTP）: 80
- メール ダウンロード（POP3）: 110

これらのプロトコルに異なるポートを使用するようにアプライアンスを設定している場合は、他の機器もそれぞれのポートを使用するように調整する必要があります。

また、アプライアンス（アプライアンスをプロキシとするプロトコル）からの内部トラフィックのみを送受信するように、ファイアウォールを設定するようにしてください。

DNS サーバのレコードの変更

組織のネットワーク トポロジとアプライアンスがプロキシするプロトコルにより、内部および外部の DNS サーバのレコードを変更する必要があります。『製品ガイド』の第 1 章にあるシナリオを参照してください。

特に、内部に FTP、Web、または POP3 サーバがある場合は、内部 FTP、Web、POP3 サーバとファイアウォールとを関連付けるレコードを外部 DNS サーバに作成する必要がある場合があります。内部 Web サーバには、Web サーバのドメイン名とその IP アドレスとを関連付けるレコードを内部 DNS サーバに作成する必要もあります。

DNS サーバに記録するレコード（およびその順番）によって、フェールオーバー、フェールクローズ、またはフェールセーフ構成（『製品ガイド』の第 1 章を参照）が実装されるかどうかが変わります。したがって、レコードが正しくリストされているかどうかを確認する必要があります。

DNS サーバ ソフトウェアの変更の詳細については、DNS サーバに添付の情報を参照してください。

設定のテスト

WebShield e500 アプライアンスがネットワークに正しく統合されていることを確認するため、次のテストを実行してください。テストの手順は、有効にしているプロキシによって異なります。

- 54 ページの「テスト 1: 電子メール メッセージ（SMTP）が正常にスキャンおよび配信されるかどうかの確認」
- 55 ページの「テスト 2: ファイル転送（FTP）時に正常にスキャンされるかどうかの確認」
- 55 ページの「テスト 3:Web ブラウズ（HTTP）時に正常にスキャンされるかどうかの確認」
- 56 ページの「テスト 4: メールのダウンロード（POP3）時に正常にスキャンされるかどうかの確認」

これらのテストには、ヨーロッパに本社を置くウイルス対策製品のベンダから構成される European Institute of Computer Anti-virus Research（EICAR）によって開発された特別なテスト ファイルを使用します。

重要 :EICAR テスト ファイルにはウィルスは*含まれていません*。他のファイルに転移、感染することはありませんし、システムに障害を与えることもありません。インストール結果のテストが終了したら、他のユーザを驚かせないように、このファイルを削除してください。

EICAR テスト ファイルを作成するコンピュータでは、テスト ファイルが削除されないように、ウィルス対策ソフトウェアが無効になっていることを確認してください。

EICAR テスト ファイルを作成するには :

1. メモ帳などの標準のテキスト エディタを開きます。
2. 必要に応じて新規テキスト ファイルを作成し、次の行を入力します。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-
ANTIVIRUS-TEST-FILE!$H+H*
```

注意 : 上記の行は、途中に改行を入れず、1 行に入力してください。

---

3. このテキスト ファイルを EICAR.COM という名前で保存します。ファイル サイズは約 70 バイトになります。

テスト 1: 電子メール メッセージ（SMTP）が正常にスキャンおよび配信されるかどうかの確認

アプライアンス SMTP ウィルス スキャンおよび配信機能をテストするには、内部メール アカウントと外部（インターネット）メール アカウント間で EICAR テスト ファイルを送信してください。

ウィルス スキャンおよび配信機能をテストするには :

1. 電子メール　アカウントのあるネットワーク上のコンピュータにログオンします。
2. EICAR テスト ファイルを作成します。
3. コンピュータの電子メール プログラムを開き、次のような新規メッセージを作成します。テストするユーザがアクセス可能なインターネット上の外部電子メール アドレスを送信先に指定し、EICAR ファイルをメッセージに添付します。
4. メッセージを送信します。

   電子メール システムが正しく設定されていて、アプライアンスがデフォルトの設定の場合、

   - メール　サーバは送信されたメッセージを内部のコンピュータから受け取り、これをアプライアンスに配信します。
   - アプライアンスはメッセージのウィルスをスキャンし、添付された EICAR テスト ファイルを検出して削除します。その後、駆除済みのメッセージを内部電子メール アカウントに返信します。
5. 返信されたメッセージに EICAR テスト ファイルが含まれていないことを確認します。
6. 最初のメッセージで指定したインターネット上の外部電子メール　アカウントにアクセスし、新しい EICAR テスト ファイルを添付した同様のメッセージを内部電子メール アカウントに送信します。

   電子メール システムが正しく設定されていて、アプライアンスがデフォルトの場合、アプライアンスは、返信メッセージを受け取り、メッセージのウィルスをスキャンし、添付された EICAR テストファイルを検出して削除します。その後、駆除済みのメッセージを外部電子メール アカウントに返信します。
7. 返信されたメッセージに EICAR テスト ファイルが含まれていないことを確認します。
8. 作成した EICAR テスト ファイルを削除します。

テスト 2: ファイル転送（FTP）時に正常にスキャンされるかどうかの確認

アプライアンスの FTP ウィルス スキャン機能をテストするには、EICAR テスト ファイルを FTP サーバに置き、それをダウンロードしてください。

FTP ウィルス スキャン機能をテストするには :

1. FTP サーバにログオンします。
2. EICAR テスト ファイルを作成します。
3. FTP クライアント（FTP ソフトウェア）のあるネットワーク上のコンピュータにログオンします。
4. コンピュータの FTP クライアントを開き、FTP サーバに接続します。
5. EICAR テスト ファイルを指定し、ダウンロードを試みます。

   FTP システムが正しく設定されていれば、アプライアンスが EICAR テスト ファイルを検知し、ダウンロードをブロックします。
6. 作成した EICAR テスト ファイルを削除します。

テスト 3:Web ブラウズ（HTTP）時に正常にスキャンされるかどうかの確認

アプライアンスの HTTP ウィルス スキャン機能をテストするには、Web サーバ上の Web ページから EICAR テスト ファイルを参照し、ダウンロードしてください。

HTTP ウィルス スキャンの機能をテストするには :

1. Web サーバにログオンします。
2. EICAR テスト ファイルを作成し、Web ページからテスト ファイルを参照します。
3. HTTP クライアント (Web ブラウザ) のあるネットワーク上のコンピュータにログオンします。
4. コンピュータの HTTP クライアントを開き、EICAR テスト ファイルを含む Web ページにアクセスします。
5. EICAR テスト ファイルをダウンロードします。

   HTTP システムが正しく設定されていれば、アプライアンスが EICAR テスト ファイルを検知し、ダウンロードをブロックします。
6. 作成した EICAR テスト ファイルを削除します。

テスト 4: メールのダウンロード（POP3）時に正常にスキャンされるかどうかの確認

アプライアンスの POP3 ウイルス スキャン機能をテストするには、メッセージに EICAR テスト ファイルを添付し、POP3 電子メール アカウントに送信します。次にメッセージをダウンロードしてください。

POP3 ウィルス スキャンの機能をテストするには :

1. POP3 サーバへのアクセスがスキャンされていないネットワーク上のコンピュータにログオンします。
2. EICAR テスト ファイルを作成し、POP3 サーバの電子メール アカウントに送信します。
3. POP3 クライアント（POP メール ダウンロード ソフトウェア）のあるネットワーク上のコンピュータにログオンします。
4. EICARテスト ファイルが添付されたPOP3電子メール アカウントのメッセージをダウンロードします。

   POP3 システムが正しく設定されていれば、アプライアンスが EICAR テスト ファイルを検知し、メッセージからテスト ファイルを削除します。
5. メッセージに EICAR テスト ファイルが含まれていないことを確認します。
6. 作成した EICAR テスト ファイルを削除します。

アプライアンスの使用方法

アプライアンスのユーザ インターフェース（x ページ）は、アプライアンスの設定をすばやく実行できるように、使いやすい設計になっています。

A ナビゲーション バー

ナビゲーション バーには、設定可能な機能が表示されています。各機能の隣には▸矢印があります。機能をクリックすると、その設定ページが開きます。

B ページ

ページにはナビゲーション バーで選択した機能の設定情報が表示されます。このページでは、これらの設定情報を変更することもできます。

注意 ：行った変更は、［**全ての変更を適用**］をクリックするまで適用されません。

各ページには次のボタンが表示されます。

製品ガイド - このボタンをクリックすると、『製品ガイド』の PDF（Portable Document Format）ファイルが表示されます。

ヘルプ - このボタンをクリックすると、現在のページのヘルプ トピックが新しいブラウザ ウィンドウに表示されます。ヘルプ トピックには、アプライアンスの機能を最適化するためのヒントなど、詳しい情報が記載されています。

キャンセル - このボタンをクリックすると、現在のページでまだ適用されていない変更が取り消されます。別のページに移動すると、Web ブラウザにページの変更が保存されるので、それらの変更をキャンセルするには、［**全ての変更をキャンセル**］を使用してください。

C パネル

いくつかのページには、追加フィールドを含むパネルがあります。ページのオプションを選択すると、パネルが表示されます。

D コントロール ボタン

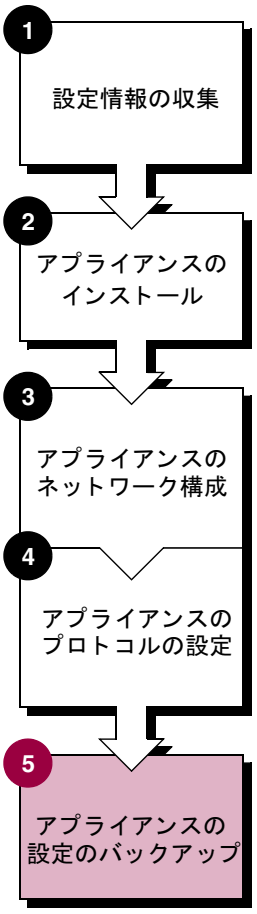
ユーザ インタフェースには、次のコントロール ボタンがあります。

- **ログオフ** ー 現在の管理セッションを終了します。このボタンをクリックすると、［ログオン］ページに戻ります。管理作業を継続するには、パスワードを入力して、アプライアンスに再度ログオンする必要があります。
- **全ての変更を適用** - アプライアンスに行った変更を適用します。
- **全ての変更をキャンセル** - 変更を最後に保存してから行ったすべてのページで行った変更をすべてキャンセルします。複数のページを変更した場合、これらの変更はすべて破棄されます。

このガイドでは、ユーザ インターフェースの各ページについて詳しく説明していません。詳細については、関連するヘルプ トピックを参照してください。

設定のバックアップと復元

アプライアンスの設定を終了したら、アプライアンスのソフトウェアに問題が発生したときにすぐに復元できるように、設定をバックアップしておくようにしてください。アプライアンスのソフトウェアを復元する方法については、61 ページの「ソフトウェアの復元とアップグレード」を参照してください。



設定のバックアップ

アプライアンスの設定を設定ファイルにバックアップするには：

1. バックアップ用の設定ファイルを作成するコンピュータで Web ブラウザを開きます。
2. 適切な URL を使用して、アプライアンスのユーザ インターフェースにアクセスし、ログオンします（35 ページの手順 2 から 38 ページの手順 7 までを参照）。
3. ナビゲーション バーで、［**システムのメンテナンス**］を選択します。
4. ［システム設定の保存］の隣の［**ファイルに保存**］をクリックします。

   ブラウザの［ファイルのダウンロード］ダイアログボックスが表示され、アプライアンスからファイルをダウンロードするかどうか確認されます。ダイアログボックスが表示されたら、［**OK**］をクリックします。

   ［名前を付けて保存］ダイアログ ボックスが開きます。
5. 設定ファイルの保存場所を選択し、必要に応じて .ZIP ファイルの名前を変更します。デフォルトは ws_cfg_backup.zip です。
6. ［**保存**］をクリックします。

   Web ブラウザによって設定ファイルが作成されます。問題がなければ、確認のダイアログボックスが表示されます。
7. 確認のダイアログボックスを閉じます。

   これで、アプライアンスの管理作業を引き続き行うことができます。

設定の復元

アプライアンスの設定を設定ファイルで復元する場合は、他の必要な変更がされていることを確認してください。例えば、複数のアプライアンスに同じ設定ファイルを使用することはできますが、異なるアプライアンスで同じ IP アドレスを使用することはできません（IP アドレスは固有）。そのため結果的に IP アドレスの変更が必要になります。

アプライアンスの以前のバージョンの設定ファイルを使用できます。アプライアンスをアップグレードする前に設定ファイルを作成した場合は、その設定ファイルを使用してアップグレードしたアプライアンスに以前の設定を復元できます。

アプライアンスの設定を設定ファイルから復元するには：

1. バックアップ用の設定ファイルがあるコンピュータで Web ブラウザを開き、適切な URL を使用して、アプライアンスのユーザ インターフェースにアクセスし、ログオンします（35 ページの手順 2 から 38 ページの手順 7 を参照）。

   既にアプライアンスのユーザ インターフェースにアクセスしていて、設定ファイルが別のコンピュータにある場合は、ファイルを使用中のコンピュータに転送してください。

2. アプライアンスの設定方法に従って、次のいずれかを行ってください。

   - 最近アプライアンスのソフトウェアの更新をした場合またはアプライアンスの初期設定をする場合は、システム設定ページに特別な設定復元パネルがあります。システム設定ページの［**設定復元**］をクリックし、このパネルにアクセスしてください。

     > **注意：**設定復元パネルは、アプライアンスの初期設定時のみ、システム設定パネルから使用可能です。

   - アプライアンスの設定が済んでいる場合は、ナビゲーション バーで［**システムのメンテナンスを選択して**］システムのメンテナンス ページを表示します。［システム設定の復元］の隣の、［**ファイル**］ボックスおよび［**URL**］ボックスを見てください。

3. ［**ファイル**］ボックスまたは［**URL**］ボックスで、設定ファイルのフルパスまたは URL を指定します。例：

   ```
   c:¥myfiles¥ws_cfg_backup.zip

   http://www.myorg.com/myfiles/ws_cfg_backup.zip
   ```

   ファイルを検索する場合は、［**参照**］をクリックします。

4. ［**すぐ復元する**］をクリックします。

   Web ブラウザによって設定ファイルが開かれ、設定がアプライアンスに送信されます。これで、アプライアンスの管理作業を引き続き行うことができます。

ソフトウェアの復元とアップグレード

アプライアンスのハードディスク ドライブのうちの 1 つに問題がある場合は、アプライアンスを稼動しながら、ドライブを別の（同じ仕様の）ドライブと交換できます。この場合、既存のドライブから置換されたドライブにディスクイメージがコピーされます。66 ページを参照してください。

しかし、アプライアンスの両方のドライブでソフトウェアの復元を行う必要がある場合があります。これは起こりそうもない状況ですが、両方のドライブを同時に外した場合に起こりえます。ソフトウェアを復元する場合には、WebShield e500 アプライアンス復旧 CD を使用します。

また、サポート担当者から WebShield e500 アプライアンス アップグレード CD が提供される場合があります。この CD には、アプライアンスのソフトウェア アップグレードが収録されています。アプライアンスのドライブをアップグレードするには、この CD を使用します。アップグレードの方法は、ソフトウェアを復元する方法と類似しています。

注意：ソフトウェアを復元またはアップグレードするときには、アプライアンスにローカルで接続する必要があります。リモートからは復元またはアップグレードすることはできません。

アプライアンスのソフトウェアを復元すると、追加でインストールしたソフトウェアも削除されます。アプライアンスとともに ePolicy Orchestrator を使用している場合には、ソフトウェアを復元した後で、ePolicy Orchestrator エージェントを再インストールする必要があります。詳細については、『コンフィグレーション ガイド』を参照してください。

アプライアンスのソフトウェアを復元またはアップデートするには :

1. アプライアンスのキーボード ポート（紫色。16 ページの F を参照）にキーボードを接続します。
2. アプライアンスのモニター ポート（16 ページの G を参照）にモニターを接続します。
3. アプライアンスの電源をオンにします（オフになっている場合）。
4. アプライアンスの復旧 CD またはアップグレード CD をアプライアンスの CD-ROM ドライブ（14 ページの B を参照）に挿入します。ソフトウェアを復元するかアップグレードするかに応じて、使用する CD が異なります。
5. 装置の前面のコントロール　パネルにあるリセット　ボタンを押します（15 ページの C を参照）。

   起動シーケンスが開始します。その後、CD が読み込まれ、使用許諾約款が表示されます。

   > **注意 :** 以下の手順は、WebShield e500 アプライアンス復旧 CD を使用している場合の手順です。画面の表示が異なる場合には、画面の指示に従ってください。

6. 使用許諾約款をよく読んでください。約款に同意する場合には Y を入力してください。

   使用許諾約款に同意しない場合（N を入力した場合）には、ソフトウェアを使用することはできません。

   次のオプションが表示されます。

   1: Perform a full installation。アプライアンスのハードディスク ドライブからすべてのデータを削除して、ソフトウェアを再インストールします。

   2: Install software on this CD。次のアイテムを含む領域を保持したまま、ソフトウェアを再インストールします。

   - 設定データ
   - ログ データ
   - 隔離された電子メール メッセージ
   - 保留された電子メール メッセージ

   復元処理でこれらの領域が保持できない場合には、領域が再作成されます。

3: Perform a software upgrade。CD を使用してソフトウェアをアップグレードします。

4: Automatic operation。上の 3 つのオプションから最適なオプションを選択して実行します。

5: Perform a full installation and stop。アプライアンスのハードディスク ドライブからすべてのデータを削除して、ソフトウェアを再インストールします。インストール完了後、CD が排出されますが、再起動は行われません。この後、アプライアンスの電源をオフにすることができます。

6: Reset passwords to factory default。アプライアンスのパスワードをデフォルトのパスワード（`e500changeme`）に戻します。

7: Do nothing and reboot。何も変更されず、CD が排出されます。アプライアンスのソフトウェアの復元またはアップグレードを実行したくないときに、誤って CD を挿入してしまった場合に、このオプションを選択してください。

7. 必要なオプションの番号を入力します。

   続行を確認するメッセージが表示されます。

8. Y を入力します。

7: Do nothing and reboot 以外を選択した場合には、復元またはアップグレード処理が開始しますステータス画面に進行状況が表示されます。選択したオプションによって異なりますが、処理は 30 分近くかかる場合があります。

警告 : 選択したオプションにより、今までの設定が失われ、アプライアンスのデフォルトの設定に戻る場合があります。

復元またはアップグレード処理が終了すると、CD が排出され、再起動されます(**5: Perform a full installation and stop** を選択した場合を除く)。起動シーケンスが終了する（約 2 分後）と、アプライアンスが使用可能な状態になります。選択したオプションによっては、アプライアンスの再設定が必要になる場合があります（35 ページを参照)。

注意 : 以前の設定を保持しないことを選択した場合または設定が保持できなかった場合には、アプライアンスのログオン後、次の点に注意してください。

- パスワードがデフォルトのパスワード（`e500changeme`）に戻されている
- LAN1 ポートの IP アドレスがデフォルトの 10.1.1.108 に戻されている
- LAN2 ポートの IP アドレスがデフォルトの 10.1.2.108 に戻されている

アプライアンスのデフォルトの設定については、『製品ガイド』の付録 A を参照してください。

トラブルシューティング

ハードウェアに関する問題

ここでは、アプライアンスのインストールと実行時に発生する可能性のある問題の解決方法について説明します。ユーザ インターフェースに関する問題の解決方法については、67 ページを参照してください。

アプライアンスに電源が供給されない

以下の点を確認してください。

- 付属の電源コードを使用してアプライアンスとコンセントを正しく接続しているかどうか。
- 電源スイッチと電源ボタンの両方がオンの位置になっているかどうか（34 ページの手順 6 を参照）。

  電源スイッチは装置の背面にあります（16 ページの E を参照）。電源ボタンは装置の前面のコントロール パネルにあります（15 ページの C を参照）。

上記の点に問題がない場合には、他の装置をコンセントに接続して、コンセントに問題がないかどうか確認してください。コンセントに問題がない場合は、アプライアンスまたは付属の電源コードに問題があります。ご購入先にご連絡ください。

アプライアンスがネットワークからトラフィックを受信しない

以下の点を確認してください。

- アプライアンスの電源がオンになっていて、ソフトウェアが稼動しているかどうか。コントロール パネルの電源 LED（15 ページの C を参照）が点灯し、ハードディスク ドライブ LED（14 ページの A を参照）がオフになっていれば、問題はありません。
- ケーブルが損傷していないかどうか。ケーブルがアプライアンスのポートと既存のネットワーク装置に正しく接続されているかどうか。アプライアンスに付属の青いケーブルを使用していない場合は、ケーブルが Cat5 UTP ストレート ケーブルかどうか確認してください。
- LAN2 ポートを既存のネットワーク装置に接続した場合、アプライアンスを透過モードで使用しているかどうか確認してください。

上記の点に問題がなければ、既存のネットワーク装置のネットワーク ケーブとネットワーク ポートに問題がないかどうか確認してください。ケーブルとポートが正常に動作している場合には、アプライアンスに問題があります。ご購入先にご連絡ください。

片方のハードディスクドライブ LED が赤く点灯している

そのハードディスク ドライブは故障しているため、交換する必要があります。

ドライブはキャディに収められているため、アプライアンスの稼動中でも欠陥のあるドライブを交換することができます。交換したドライブのディスク イメージは、既存のドライブから自動的に作成されます。

警告：ハードディスク ドライブを交換する場合は、必ず以下の情報に従ってください。

- いかなる場合でも両方のディスクを同時に取り外さないでください。少なくとも 1 つのドライブが、常にアプライアンスに残っている必要があります。
- 片方のドライブを取り外した状態で、数分以上アプライアンスを稼動させないでください。空気の流れを妨げる原因となり、それによってアプライアンスがオーバーヒートする可能性があります。交換用ドライブを速やかに挿入してください。
- 既存のドライブと全く同じ仕様のドライブのみを使用してください。
- ドライブを取り扱うとき、静電気に敏感なコンポーネントに手を触れないように注意してください。十分な帯電防止対策をとり、手やその他の物をアプライアンスの空のドライブ領域に入れないでください。

故障したドライブを交換するには：

1. 故障したドライブの取り出しボタンを押して、ドライブのハンドルを引き下げます（図 4-5 を参照）。ドライブ領域からドライブを引き出します。

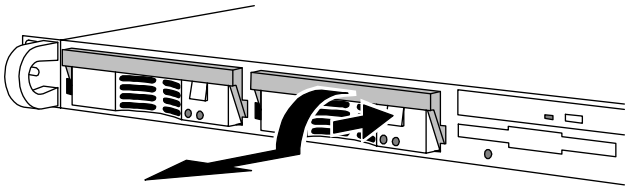


図 4-5. ドライブの取り外し

2. 交換用ドライブを空のドライブ領域に挿入し、ハンドルを押し上げてドライブを固定します（図 4-6 を参照）。

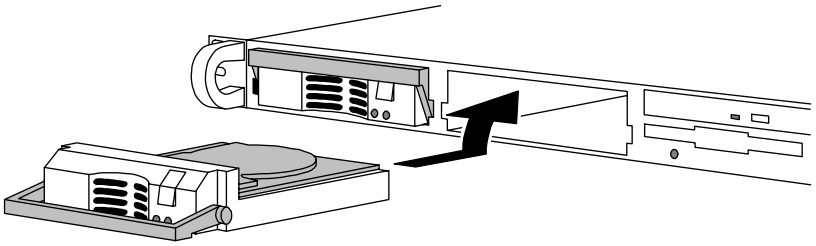


図 4-6. ドライブの挿入

アプライアンスが既存ドライブから交換したドライブにイメージをコピーします。コピーには 20 分から 30 分かかります。コピー中は交換したドライブの緑の LED が点滅します。

両方のハードディスクドライブ LED が赤く点灯している

アプライアンスのドライブに問題があります。WebShield e500 アプライアンス復旧 CD を使用して、アプライアンスのソフトウェアを復元してください（61 ページを参照）。問題が解決しない場合には、ご購入先までお問い合わせください。

ユーザ インターフェースに関する問題

ここでは、ユーザ インターフェースでアプライアンスを設定する場合に発生する可能性のある問題の解決方法について説明します。

[ログオン] ページにアクセスできない

以下の点を確認してください。

- アプライアンスの電源がオンになっていて、ソフトウェアが稼動しているかどうか。コントロール パネルの電源 LED（15 ページの C を参照）が点灯し、ハードディスク ドライブ LED（14 ページの A を参照）がオフになっていれば、問題はありません。
- Web ブラウザの URL フィールドで、`http` ではなく `https` を使用しているかどうか。ブラウザが Secure Sockets Layer（SSL）v3.0 による暗号化をサポートし、これが有効になっているかどうか。
- アプライアンスの管理に使用しているコンピュータで、そのコンピュータのプロキシとしてアプライアンスが設定されていないかどうか。管理用コンピュータとアプライアンスの間にプロキシが存在する場合は、そのプロキシはアプライアンスのハンドオフ ホストとして設定されていなければなりません。

- アプライアンスの LAN1 ポート（17 ページの H を参照）を通して、ネットワーク経由でアプライアンスにリモート接続している場合は、以下の点について確認してください。

  – 使用しているコンピュータが正常にネットワークに接続されていて、アプライアンスが接続されているサブネットに到達できるかどうか。

  – LAN1 ポートに新規に設定した IP アドレスを Web ブラウザの URL フィールドで使用しているかどうか。デフォルトの IP アドレス（10.1.1.108）を削除または無効にしていない場合は、この IP アドレス（https://10.1.1.108）を使用してみてください。

    アプライアンスの IP アドレスは、アプライアンスが接続されているサブネットで有効なアドレスでなければなりません。そうでない場合には、デフォルト IP アドレスを試してください。それが失敗した場合には直接管理接続（32 ページの手順 4）を試してください。

    注意 ：プロキシ モードでアプライアンスを使用していてさらに LAN2 ポートを無効にしていない場合のみ（40 ページの手順 17）、LAN2 ポートを通した直接管理接続が可能です。

  – アプライアンスが既存のネットワークに正常に接続されているかどうか。NIC 1 ネットワーク アクティビティ LED （コントロール パネル、15 ページの C を参照）の点滅によって確認できます。

    LED が点滅していない場合には、ケーブルが損傷していないかどうか。ケーブルがアプライアンスの LAN1 ポートと既存のネットワーク装置に正しく接続されているかどうか。アプライアンスに付属の青いケーブルを使用していない場合は、ケーブルが Cat5 UTP ストレート ケーブルかどうか確認してください。

- アプライアンスがプロキシ モードで動作していて、LAN2 ポート (18 ページの I を参照) を通して直接的なローカル管理接続をしている場合は、以下の点について確認してください。

  – LAN2 ポートが無効になっていないかどうか。これを確認するには、リモート接続を行う必要があります。

  – LAN2 ポートに新規に設定した IP アドレスを Web ブラウザの URL フィールドで使用しているかどうか（デフォルトの IP アドレスは 10.1.2.108 です）。

– アプライアンスがコンピュータに正常に接続されているかどうか。NIC 2 ネットワーク アクティビティ LED（コントロールパネル、15 ページの C を参照）の点滅によって確認できます。

  LED が点滅していない場合には、ケーブルが損傷していないかどうか。ケーブルがアプライアンスの LAN2 ポートとコンピュータのネットワーク ポートに正しく接続されているかどうか。アプライアンスに付属のオレンジ色のケーブルを使用していない場合は、ケーブルが Cat5 UTP クロス ケーブルかどうか確認してください。

[ログオン] ページは表示されるが、[ログオン] ボタンの表示が「初期化中」となっている

アプライアンスがユーザ インターフェースに必要なコンポーネントが Web ブラウザに存在するかどうかを確認しています。

アプライアンスは、Internet Explorer v 5.5 または v6.0 用に最適化され、それ以外のバージョンまたは Netscape Navigator はサポートしていません。ＩＥ v 5.5 または v6.0 以外の Web ブラウザを使用している場合は、ユーザ インターフェースにアクセスできず、アプライアンスを設定できない可能性があります。

アプライアンスのユーザ インターフェースには Java2 ランタイム環境が必要なため、このソフトウェアをブラウザにインストールしている可能性があります。この環境を Web ブラウザにインストールする場合には、ブラウザで必要とするコンポーネントに応じて、5 ～ 14MB の空き容量が必要になります。また、速度の遅いリモート回線を使用している場合には、インストールにかかる時間が長くなります。

パスワードが使用できない

以前の設定を使用せずにアプライアンスのソフトウェアを復元すると、パスワードはデフォルトのパスワード（`e500changeme`）に戻ります。

パスワードを忘れてしまった

WebShield e500 アプライアンス復旧 CD を使用して、アプライアンスのパスワードをデフォルトの `e500changeme` に戻す必要があります。61 ページの「ソフトウェアの復元とアップグレード」を参照してください。復旧プロセスで **6: Reset passwords to factory default** を選択してください。

一部のユーザ インターフェースが正しく表示されない

アプライアンスのユーザ インターフェースは Microsoft Internet Explorer v4.0、v5.0、v5.5、または v6.0 用に最適化され、Netscape Navigator v4.7 をサポートしています。製品に付属の『リリース ノート』で、特定のオペレーティング システムで Web ブラウザを使用した場合の問題について確認してください。

クライアント（ソフトウェア）がアプライアンス経由で通信できない。

以下の点を確認してください。

- 必要なプロキシがアプライアンスで有効になっているかどうか。サポートされているプロトコルは、初期設定ですべて有効になっています。44 ページの「プロトコルの設定」を参照してください。
- クライアントとその他の装置が、トラフィックをアプライアンスに送信する、またはアプライアンスから受信するようにルーティングが設定されているかどうか。51 ページの「他の機器の設定」を参照してください。
- ネットワークに問題がなく、装置が正しく接続されているかどうか。

Web が参照できない、または URL ブロックが実行されない

URL ブロックが設定されている場合、アプライアンスが DNS サーバにアクセスできないと、Web ブラウズ（HTTP）要求を受信したときに URL をブロックするかどうか決めることができません。したがって、［システム設定］ページで DNS サーバを設定する必要があります。38 ページの手順 9 を参照してください。